Zusammenfassung M145

Netzwerk betreiben und erweitern

Emanuel Duss

2011-11-28

Informationen

Autor	Emanuel Duss
Erstellt am	2008-09-01
Bearbeitet am	2011-11-28
Erstellt mit	OpenOffice.org auf Ubuntu Linux

Lizenz

Bearbeitungsprotokoll

Datum	Version	Änderung
2008-09-91	0.1	Erstellt
2010-05-15	1	Final
2011-11-28	1.1	Kleine Bereinigung

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Problembehandlung

1.1 Häufige Netzwerkprobleme

Hardware-Fehler

- Beschädigung oder Veraltung der Kabel
- Hardware-Komponenten eines Endgeräts
- Fehlerhafte aktive Netzwerkkomponente
- Probleme mit Komponenten eines Servers
- Ausfall der Stromversorgung

Software-Fehler

- Konfiguration am Endgerät
- Konfiguration bei Server und Diensten
- Falsch konfigurierte Switches und Router

Benutzerfehler

- Fehlbedienung der Hardware
- Fehlbedienung der Software
- Installation neuer Software
- Änderungen an der Computer-Konfiguration
- Attacken auf das Netzwerk und seine Komponenten

Dagegen kann man folgendes machen:

- Schulen
- Entzug von Rechten

Unzureichende Netzwerkleistung

- Aktive Netzwerkkomponenten sind dem Datenverkehr nicht gerecht
- Komponenten oder Server oder Dienste sind überlastet
- Falsche Konfiguration der Protokolle
- Netzwerkarchitektur entspricht nicht den aktuellen Anforderungen
- Es werden zu viele Daten übertragen (Broadcast)

1.1 Netzwerkserver überwachen

Task-Manager und Systemmonitor überwachen folgende Sachen (wichtige Auswahl):

- Prozessorauslasgun, Festplattenaktivität, Auslastung des Arbeitsspeichers, Netzwerkauslastung
- Grafische Darstellung ist gut
- Leistungsprotokoll speichern
- Aktivität des Servers protokollieren
- Man erkennt in welchen Zeitraum immer die selben Probleme kommen (z.B. Am Morgen beim Anmelden)

1.1.1 Aktive Netzwerkkomponente überwachen

- SNMP (Simple Network Management Protocol): SNMP-Manager fragt den SNMP-Agenten um Informationen über die aktive Netzwerkkomponente.
- Rückmeldung kommt als Trap-Meldung.
- Netzwerkpakete mit einem Netzwerkmonitor z.B: Wireshark oder tcpdump auswerten.
- Statistik und der Inhalt kann angezeigt werden.

1.1.1 Wege zur Fehlerermittlung

- Digitales Multimeter
- Spannung und Wiederstand messen
- Abschirmung!
- Oszilloskop
- Zeitliche Veränderung der Spannung
- Kabeltester und erweiterter Kabeltester
- LAN-Messgerät (Time Domain Reflectometer)
- Protocollanalysator

1.1.1 Netzwerkkarte

ping localhost prüft, ob die Netzwerkkarte ordnungsgemäss installiert ist.

1.2 Systemmonitor (Windows)

Wozu dient der Systemmonitor?

- Analyse und Protokollierung der Aktivität eines Computers
- Überwacht verschiedene Leistungsobjekte (Prozessor, Speicher, Netzwrekschnittstelle)
- Auswertung in Form von: Diagramm, Warnung oder Protokoll
- Gestartet wird der Systemmonitor (Leistung) über perfmon.msc.

2 Grundlegendes

2.1 TCP/IP-Referenzmodell

TCP/IP-Schicht	≈ OSI-Schicht	Beispiel
Anwendungsschicht	5–7	HTTP, FTP, SMTP, POP, Telnet
Transportschicht	4	TCP, UDP, SCTP
Internetschicht	3	IP (IPv4,IPv6)
Netzzugangsschicht	1–2	Ethernet, Token Bus, Token Ring, FDDI

Tabelle 1: TCP/IP-Referenzmodell

2.2 Netzwerk-Protokolle

2.2.1 Nicht routbare Protokolle

Pro	Kontra
• Schnell bei weniger als 30 Geräten • Nur im gleichen Subnetz • Einfache Konfiguration	• Nicht Routbar • Nur für Windows • Nicht für Internetzugriff geeignet

Beispiele: NetBIOS / NetBEUI

2.2.2 Routbare Protokolle

Pro	Kontra
• Geeignet für grosse LANs und WANs • Routbar über Router, Subnetze, Internet • Betriebssystemunabhängig • Heutiges Standardprotokoll	• Zu viel Overhead bei kleinen Netzen • schwierige Konfiguration in grösseren Netzen • Braucht Hilfsmittel wie Host-File, DNS, WINS

Beispiel: TCP/IP

2.2.3 TCP/IP

- Ipv4 ist heutiger Standard
- Verwendung wenn: Routbar, Internetzugriff und andere Betriebssysteme

2.3 ISO/OSI-Referenzmodell

#	Layer EN	Layer DE		Funktion		Adressierung	Einheiten	Protokolle	HW
7	Application	Applikation	Anwendungsorientiert	Netzwerktransparenz für User. Netwerkmanagement. Bereitstellung von Diensten.	Hardware unabhängig		Daten	HTTP, FTP, DNS, SMTP, POP3, NetBIOS, LDAP	Gateway, Content-Switch, Layer-4-7-Switch
6	Persentation	Darstellung		Konvertierung der ausgetauschten Daten in eine systemunabhängige Form (Umsetzung der Syntax) zur Sicherstellung der wechselseitig richtigen Interpretation. Datenkompression				HTML / XML	
5	Session	Sitzung		Auf- und Abbau einer Dialogverbindung (Login auf Webpage). Steuerung des Dialogs: wer wann wie lange sendet. Setzen von Synchronisationspunkten				SMB	
4	Transport	Transport	Transportorientiert	Unterstützung einer zuverlässigen Ende-zu-Ende-Verbindung zwischen Prozessen (Transportdienstbenutzer) auf den Endsystemen. Formelle Aushandlung der Verbindungsbeziehung zwischen Client und Server (über Port). Fehlerkontrolle bei TCP.		Portnummer	Segmente	TCP, UDP, SCTP, SPX	Firewall
3	Network	Vermittlung		Weiterleitung der Datenpakete zwischen den einzelnen Netzwerken (WAN, Internet). Adressierung von Computern mit IP-Adressen. Routing von Daten. Adressierung von PCs mit IP-Adressen. Umsetzung von HW-Adressen in IP-Adressen.		IP-Adresse	Pakete	IP-Protocol ARP ICMP, IGMP, IP, IPX NetBEUI	Router, Layer-3-Switch
2	Data Link	Sicherung		Aufteilung der Bitströme in Frames. Behandlung von Übertragungsfehlern. Regelung des Zugriffs auf das gemeinsam genutzte Übertragungsmedium. Sublayer: LLC und MAC	Hardwareabhängig	MAC-Adresse	Rahmen (Frames)	ARP Ethernet (IEEE 802.3), WLAN (IEEE 802.11), Token Ring, FDDI, ARCNET	Switch, Bridge
1	Physical	Bitübertragung		Übertragung von Bitströmen; Festlegung einer Übertragungsrate für die Bitsynchronisation; Darstellung der Bits mit Leitungscodes (elektrische oder optische Signale)			Bits	Kabeltypen,Übertragungsraten	Hub, Repeater

Tabelle 2: ISO/OSI-Referenzmodell

3 IP-Rechnen

3.1 Subnetzmasken

Hostanzahl	Subnetzmaske	Binär (32 Bit)	Präfix
16.777.214	255.0.0.0	1111 1111 0000 0000 0000 0000 0000 0000	/8
8.388.606	255.128.0.0	1111 1111 1000 0000 0000 0000 0000 0000	/9
4.194.302	255.192.0.0	1111 1111 1100 0000 0000 0000 0000 0000	/10
2.097.150	255.224.0.0	1111 1111 1110 0000 0000 0000 0000 0000	/11
1.048.574	255.240.0.0	1111 1111 1111 0000 0000 0000 0000 0000	/12
524.286	255.248.0.0	1111 1111 1111 1000 0000 0000 0000 0000	/13
262.142	255.252.0.0	1111 1111 1111 1100 0000 0000 0000 0000	/14
131.070	255.254.0.0	1111 1111 1111 1110 0000 0000 0000 0000	/15
65.534	255.255.0.0	1111 1111 1111 1111 0000 0000 0000 0000	/16
32.766	255.255.128.0	1111 1111 1111 1111 1000 0000 0000 0000	/17
16.382	255.255.192.0	1111 1111 1111 1111 1100 0000 0000 0000	18
8.190	255.255.224.0	1111 1111 1111 1111 1110 0000 0000 0000	/19
4.094	255.255.240.0	1111 1111 1111 1111 1111 0000 0000 0000	/20
2.046	255.255.248.0	1111 1111 1111 1111 1111 1000 0000 0000	/21
1.022	255.255.252.0	1111 1111 1111 1111 1111 1100 0000 0000	/22
510	255.255.254.0	1111 1111 1111 1111 1111 1110 0000 0000	/23
254	255.255.255.0	1111 1111 1111 1111 1111 1111 0000 0000	/24
126	255.255.255.128	1111 1111 1111 1111 1111 1111 1000 0000	/25
62	255.255.255.192	1111 1111 1111 1111 1111 1111 1100 0000	/26

30	255.255.255.224	1111 1111 1111 1111 1111 1111 1110 0000	/27
14	255.255.255.240	1111 1111 1111 1111 1111 1111 1111 0000	/28
6	255.255.255.248	1111 1111 1111 1111 1111 1111 1111 1000	/29
2	255.255.255.252	1111 1111 1111 1111 1111 1111 1111 1100	/30

3.2 Private IP-Adressen (RFC 1918)

Nach RFC 1918 können folgende IP-Adresse für private Zwecke verwendet werden:

Netzadressbereich	CIDR-Notation	Anzahl Addr	Anzahl Netze gemäss Netzklasse (historisch)
10.0.0.0 - 10.255.255.255	10.0.0.0/8	2^{24} = 16.777.216	Klasse A: 1 Netz mit 16.777.216 Adressen: 10.0.0.0/8
172.16.0.0 - 172.31.255.255	172.16.0.0/12	2^{20} = 1.048.576	Klasse B: 16 Netze mit je 65.536 Adressen: 172.16.0.0/16 - 172.31.0.0/16
192.168.0.0 - 192.168.255.255	192.168.0.0/16	2^{16} = 65.536	Klasse C: 256 Netze mit je 256 Adressen: 192.168.0.0/24 - 192.168.255.0/24

3.3 Netzklassen

Netzklassen werden heutzutage nicht mehr verwendet, obwohl diese am BBZWITS unterrichtet werden. Netzklassen sind unflexibel und wenig sparsam. Sie verwirren nur und werden in der Praxis nicht mehr eingesetzt.

IP-Klassen wurden im Jahr 1993 per RFC 1518 und RFC 1519 durch das Classless Inter-Domain-Routing ersetzt. Bei CIDR werden innerhalb des gesamten Adressraumes Netze in flexiblen Grössen vergeben, folglich ist eine Ableitung der Netzgrösse aus der IP-Adresse nicht mehr möglich. Leider gib es immer noch Lehrer, die Netzklassen verwenden und unterrichten, wie z.B. am BBZWITS.

Klasse	Präfix	Adressbereich	Netzmaske	Netzlänge (mit Präfix)	Netzlänge (ohne Präfix)	Hostlänge	Netze	Hosts pro Netz
A	0...	0.0.0.0 – 127.255.255.255	255.0.0.0	8 Bit	7 Bit	24 Bit	128	16.777.214
B	10...	128.0.0.0 – 191.255.255.255	255.255.0.0	16 Bit	14 Bit	16 Bit	16.384	65.534
C	110...	192.0.0.0 – 223.255.255.255	255.255.255.0	24 Bit	21 Bit	8 Bit	2.097.152	254
D	1110...	224.0.0.0 – 239.255.255.255	Verwendung für Multicast-Anwendungen					
E	1111...	240.0.0.0 –	reserviert (für experimentelle Zwecke)					

	255.255.255.25 5

3.4 IP#-Rechnen mit der ultimativen Master Table! Yay!

3.4.1 Master-Table

Anzahl Bit	0	1	2	3	4	5	6	7	8
Dezimal	0	128	192	224	240	248	252	254	255
Binär	00000000	10000000	11000000	11100000	11110000	11111000	11111100	11111110	11111111
Klasse	A	B	C	D	E				
Kuchenstückgrösse	256	128	64	32	16	8	4	2	1
Wie viele Stücke?	1	2	4	8	16	32	64	128	256

3.4.2 Ablesen

1. **Alternative Schreibweise der Subnetzmask**e lässt sich mit Hilfe der Dezimalen Schreibweise und den Anzahl Bits ablesen.
2. Die **Klasse** kann man mit Hilfe der Dezimalen Schreibweise und der IP-Klasse ablesen. A geht von 0 bis (ohne mit) dort wo B anfängt.
3. Bei der **Anzahl mögliche Hosts im Subnetz:** $2^{\text{32-Alternative Schreibweise}}$ -2 oder $2^{\text{Anzahl Host-Bits}}$ -2. Das -2 kommt davon, weil man die Netz-ID und Broadcasts abgezogen wird.
4. **Anzahl mögliche Subnetze mit gleicher Maske**:
   $2^{\text{Wie viele Bits wurden zusätzlich zur Adressklasse gesetzt?}}$ (evtl. -2) oder $2^{\text{Anzahl Netzwerk Bits – Anzahl Bits der Klasse}}$ (evtl. -2)
   Das „evtl -2“ muss gemacht werden, weil dies der Lehrer so will. Dies hat man früher (vor unserer Geburt) so gemacht und vielleicht treffen wir mal so ein Router an...
5. **Netz-ID**: Wie gross ist die Kuchenstückgrösse? Dann rechnet man dort wo die Subnetzmaske ungerade wird die **IP-Adresse durch die Kuchenstückgrösse**. Dann **rechnet man ohne Rest zurück**. Dann hat man den Teil der Netz-ID. Man schreibt also dort wo die Subnetzmaske 255 ist das selbe wie bei der IP-Adresse hin. Dort wo die Subnetzmaske ungerade ist schreibt man das ausgerechnete hin und dort wo die Subnetzmaske 0 ist, schreibt man eine 0 hin.
6. **Broadcast-Adresse**: Man rechnet zur Netz-ID die Kuchenstückgrösse hinzu und erhält den Anfang vom nächsten Subnetz. Dann nimmt man 1 Bit weg. Also die grösste Adresse im ganzen Bereich.
7. **Host-ID**: Man rechnet den Teil der IP-Adresse (dort wo die Subnetzmaske ungerade ist) minus den „ungeraden“ Teil der Netz-ID. Dort wo die Subnetzmaske bei der IP-Adresse ungerade ist, übernimmt man genau das selbe. Der vordere Teil (also dort wo die Subnetzmaske gerade ist) lässt man einfach weg. ODER: Um die wie vielte IP-Adresse handelt es sich? z.B: Bei 77.88.99.235 // 255.255.240.0 wäre es 3.235. Der Teil wo sie IP-Adresse 255 ist, kann man weglassen. Bei 0 bleibt der Teil wie er ist. Es wird nur das „ungrade“ bereücksichtigt. Bei der Host-ID schaut man auf die IP-Adresse und auf die Netz-ID!!!

3.5 Supernetting / Summieren / Summarizing

Damit kann man mehrere Routing-Tabellen-Einträge zu einem Eintrag zusammenfassen.

- Man erstellt eine Tabelle: [Netzwerkadresse] [Subnetzmaske] [Start- und End-IP]
- Entsteht ein zusammenhängender Bereich **ohne Lücken**? Falls JA, schreibt man diesen Bereich hin.

<table>
<tr><td>160 – 164</td><td>164 – 168</td><td>168 – 172</td><td>172 – 176</td></tr>
<tr><td colspan="2">160 – 168</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>170-176</td></tr>
<tr><td colspan="4">160 – 176
(Netz, das alle anderen beinhaltet!)</td></tr>
</table>

4 Layer 2: Ethernet-Frame

4.1 Aufbau Ethernet II Frame (Ethernet DIX)

Das DIX-Konsortium standardisierte die Darstellung von Ethernet-Frames. Diese nennt man auc Ethernet II Frames.

Destination Address	Source Address	Type	Data / Nutzlast
6 Byte	6 Byte	2 Byte	64 bis 1518 Byte
Ethernet II Header			Data

4.1.1 MAC-Adressen Aufbau

I/G	U/L	Hersteller	Karten-ID
1 Bit	1 Bit	22 Bit	24 Bit
48 Bit = 6 Byte			

- I = 0 = Individuell = Unicast
- G = 1= Gruppe = Multicast oder Broadcast
- U = 0= Universell = von IEEE-OUI Konvention erzeugte Adresse
- L = 1 = Lokale Adresse = nur lokal verwendbar (durch Software erzeugte MAC-Adresse, die sich nicht an die OUI Einteilung der IEEE hält

Unicast	Zustellung an ein Ziel
Multicast	Zustellung an mehrere Ziele (Streaming, Spanning Tree Protocol (STP), IRC)
Broadcast	Zustellung an alle Hosts innerhalb der gleichen Broadcast-Domäne

Unicast: 00:45:A9:A8:F1:69; genau ein Ziel

Broadcast: FF:FF:FF:FF:FF:FF; geht an alle

4.1.2 Ether-Type

Zu welchem Layer 3-Protokoll gehört die zu transportierende Nutzlast?

IANA legt diese fest:

Ether-Type	**Layer 3 Protokoll**
0x0800	IP
0x0806	ARP
0x8100	VLAN tagged Frames
0x8035	Reverse ARP (RARP)
0x8138	Novell
0x86DD	IPv6

Tabelle 3: Ethernet-Types

5 Layer 3: IP-Paket[1]

5.1 Das IP-Paket

Auf der Internetschicht des TCP/IP-Protokollstapels, auf der das IP-Protokoll arbeitet, werden die Datenpakete, wie bereits erwähnt, als Datagramme bezeichnet. Um die Datenübertragung mithilfe des IP-Protokolls genau zu erläutern, soll an dieser Stelle zunächst der IP-Header vorgestellt werden. Er enthält die Steuerdaten, die das IP-Protokoll zu einem Datenpaket hinzufügt, das ihm vom übergeordneten Transportprotokoll übergeben wird.

Der IPv4-Protokoll-Header wird wie das gesamte Protokoll in RFC 791 definiert. Seine Länge beträgt mindestens 20 Byte, dazu können bis zu 40 Byte Optionen kommen.

Byte	0		1	2		3
0	Version	IHL	Type of Service	Paket-Gesamtlänge		
4	Identifikation			Flags	Fragment-Offset	
8	Time to Live		Protokoll	Header-Prüfsumme		
12	Quell-Adresse					
16	Ziel-Adresse					
20	Optionen					Padding
...	evtl. weitere Optionen					

- **Version** (4 Bit): Die Versionsnummer des IP-Protokolls, die das Paket verwendet. Bei IPv4, wie der Name schon sagt, die Version 4.
- **IHL** (4 Bit): Internet Header Length; die Länge des Internet-Headers in 32-Bit-Worten (entsprechen den Zeilen in der obigen Tabelle). Der kleinste mögliche Wert beträgt 5.
- **Type of Service** (8 Bit): Ein Code, der die Art des Datenpakets bestimmt. Bestimmte Sorten von Paketen, etwa für den Austausch von Routing- oder Status-Informationen, werden von bestimmten Netzen bevorzugt weitergeleitet. In ihrem 1999er-Aprilscherz bot die Computerzeitschrift c't ein angebliches Tool zum Download an, das diese Quality-of-Service-Informationen manipulieren könne, um die Geschwindigkeit von Internet-Verbindungen zu erhöhen. [Die Satire war immerhin so überzeugend gemacht, dass ein Leser per empörtem Leserbrief sein Abo kündigte, weil er mit derart »unmoralischem Verhalten« im Netz nichts zu tun haben wollte.]
- **Paket-Gesamtlänge** (16 Bit): Die Gesamtlänge des Datagramms in Bytes, Header und Nutzdaten.
- **Identifikation** (16 Bit): Ein durch den Absender frei definierbarer Identifikationswert, der beispielsweise das Zusammensetzen fragmentierter Datagramme ermöglicht.
- **Flags** (3 Bit): Kontrollflags, die die Paketfragmentierung regeln. Das erste Bit ist reserviert und muss immer 0 sein, das zweite (DF) bestimmt, ob das Paket fragmentiert werden darf (Wert 1) oder nicht (0), das dritte (MF) regelt, ob dieses Paket das letzte Fragment (0) ist oder ob weitere Fragmente folgen (1).

1 Quelle: Galileo Computing: IT-Handbuch für Fachinformatiker (ISBN 978-3-8362-1015-7)

- **Fragment-Offset** (13 Bit): Dieser Wert (angegeben in 64-Bit-Blöcken) legt fest, an welcher Stelle in einem Gesamtpaket dieses Paket steht, falls es sich um ein Fragment handelt. Das erste Fragment oder ein nicht fragmentiertes Paket erhält den Wert 0.
- **Time to Live** (8 Bit): Der TTL-Mechanismus sorgt dafür, dass Datagramme nicht endlos im Internet weitergeleitet werden, falls die Empfängerstation nicht gefunden wird. Jeder Router, der ein Datagramm weiterleitet, zieht von diesem Wert 1 ab; wird der Wert 0 erreicht, leitet der betreffende Router das Paket nicht mehr weiter, sondern verwirft es.
- **Protokoll** (8 Bit): Die hier gespeicherte Nummer legt fest, für welches Transportprotokoll der Inhalt des Datagramms bestimmt ist. Die beiden wichtigsten Transportprotokolle (TCP und UDP) werden im nächsten Abschnitt beschrieben.
- **Header-Prüfsumme** (16 Bit): Die Prüfsumme stellt eine einfache Plausibilitätskontrolle für den Datagramm-Header zur Verfügung. Ein Paket, dessen Header-Prüfsumme nicht korrekt ist, wird nicht akzeptiert und muss erneut versendet werden.
- **Quelladresse und Zieladresse** (je 32 Bit): Die IP-Adressen von Absender und Empfänger. IP-Adressen wurden oben ausführlich behandelt.
- **Optionen** (variable Länge): Die meisten IP-Datagramme werden ohne zusätzliche Optionen versandt, da Absender- und Empfänger-Host sowie alle auf dem Weg befindlichen Router die jeweils verwendeten Optionen unterstützen müssen. Zu den verfügbaren Optionen gehören unter anderem Sicherheitsfeatures und spezielle Streaming-Funktionen.

Quelle: Wikipedia

5.1.1 Protocol-Types

Protocol	Layer 4 Protokoll
1	ICMP
4	IP (für IP-in-IP)
6	TCP
17	UDP
50	ESP
51	AH

Tabelle 4: Protocol-Types

6 Layer 4: Transportschicht (TCP und UDP)

6.1 TCP – Transmission Control Protocol

6.1.1 Eigenschaften

- Verbindungsorientiert / Verbindngsmanagement
  - Verbindung muss aufgebaut werden
  - Periodische Keep-Alive-Prozesse überprüfen, ob die Verbindung noch steht
  - Verbindung wird über beide Partner beendet
  - End-zu-End Verbindung
- Flusskontrolle
  - Vollduplex: Eingehender und ausgehender Kanal
- Zuverlässig
  - Jedes Paket erhält eine Sequenznummer
  - Jedes Paket wird bestätigt (wenn keine Bestätigung erfolgt, wird das Paket erneut gesendet)
- Zeitüberwachung
- Streaming ist nicht möglich!

6.1.2 TCP-Header

Das TCP-Paket wird im IP-Datagramm eingekapselt: Ethernet(IP(TCP()))

<table>
<tr><td colspan="1">0</td><td colspan="1">1</td><td colspan="1">2</td><td colspan="1">3</td><td colspan="1">4</td><td colspan="1">5</td><td colspan="1">6</td><td colspan="1">7</td><td colspan="1">8</td><td colspan="1">9</td><td colspan="1">10</td><td colspan="1">11</td><td colspan="1">12</td><td colspan="1">13</td><td colspan="1">14</td><td colspan="1">15</td><td colspan="1">16</td><td colspan="1">17</td><td colspan="1">18</td><td colspan="1">19</td><td colspan="1">20</td><td colspan="1">21</td><td colspan="1">22</td><td colspan="1">23</td><td colspan="1">24</td><td colspan="1">25</td><td colspan="1">26</td><td colspan="1">27</td><td colspan="1">28</td><td colspan="1">29</td><td colspan="1">30</td><td colspan="1">31</td></tr>
<tr><td colspan="16">Source port</td><td colspan="16">Destination port</td></tr>
<tr><td colspan="32">Sequence number</td></tr>
<tr><td colspan="32">Acknowledgment number</td></tr>
<tr><td colspan="4">Data offset</td><td colspan="4">Reserved</td><td>CWR</td><td>ECE</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="16">Window Size</td></tr>
<tr><td colspan="16">Checksum</td><td colspan="16">Urgent pointer</td></tr>
<tr><td colspan="32">Options (if Data Offset > 5)
...</td></tr>
</table>

Ohne 'Options and padding' und 'Data' ist der TCP-Header 20 Bytes gross.

Erläuterung der Felder

Feld	Beschreibung
Source Port	Quellport: Gibt die Portnummer auf der Senderseite an.
Destination Port	Zielport: Gibt die Portnummer auf der Empfängerseite an.
Sequence Number	Sequenznummer des ersten Daten-Oktetts (Byte) dieses TCP-Paketes oder die Initialisierungs-Sequenznummer falls das SYN-Flag gesetzt ist. Nach der Datenübertragung dient sie zur Sortierung der TCP-Segmente, da diese in unterschiedlicher Reihenfolge beim Empfänger ankommen können.
Acknowledgment Number	Quittierungsnummer: Sie gibt die Sequenznummer an, die der Sender dieses TCP-Segmentes als nächstes erwartet. Sie ist nur gültig, falls das ACK-Flag gesetzt ist.
Data Offset	Länge des TCP-Headers in 32-Bit-Blöcken – ohne die Nutzdaten (Payload). Hiermit wird die Startadresse der Nutzdaten angezeigt.
Reserved	Das Reserved-Feld wird nicht verwendet und muss Null sein.
Control-Flags	sind zweiwertige Variablen, mit den möglichen Zuständen gesetzt und nicht gesetzt, welche zur Kennzeichnung bestimmter für die Kommunikation und Weiterverarbeitung der Daten wichtiger Zustände benötigt werden. Im folgenden werden die Flags des TCP-Headers und die von ihrem Zustand abhängigen, auszuführenden Aktionen beschrieben.
URG	Ist das Urgent-Flag (urgent = dringend) gesetzt, so werden die Daten, auf die das Urgent-Pointer-Feld zeigt, sofort von der Anwendung bearbeitet. Dabei unterbricht die Anwendung die Verarbeitung der Daten des aktuellen TCP-Segments und liest das Byte aus, auf das der Urgent-Pointer zeigt. Dieses Verfahren ist fern verwandt mit einem Softwareinterrupt. Dieses Flag kann zum Beispiel verwendet werden, um eine Anwendung auf dem Empfänger abzubrechen. Das Verfahren wird nur äußerst selten benutzt, Beispiele sind rlogin und telnet. **ACK**: Das Acknowledgment-Flag hat in Verbindung mit der Acknowledgment-Nummer die Aufgabe, den Empfang von TCP-Segmenten beim Datentransfer zu Bestätigen. DieAcknowledgment-Nummer ist nicht gültig, wenn das Flag nicht gesetzt ist. **PSH**: Das Push-Flag hat die Aufgabe, die Daten unter Umgehung des Puffers, eines Speichers für die Zwischenlagerung von Daten, sofort an die Anwendung weiterzuleiten. Hilfreich ist dies, wenn man zum Beispiel bei einer Telnet-Sitzung einen Befehl an den Empfänger senden will. Würde dieser Befehl erst im Puffer zwischengespeichert werden, so würde dieser (stark) verzögert abgearbeitet werden. **RST**: Das Reset-Flag wird verwendet, wenn eine Verbindung abgebrochen werden soll. Dies geschieht zum Beispiel bei technischen Problemen oder zur Abweisung unerwünschter Verbindungen. **SYN**: Pakete mit gesetztem SYN-Flag initiieren eine Verbindung. Der Server antwortet normalerweise entweder mit SYN+ACK, wenn er bereit ist, die Verbindung anzunehmen, andernfalls mit RST. Dient der Synchronisation von Sequenznummern beim Verbindungsaufbau (daher die Bezeichnung SYN). **FIN**: Dieses Finish-Flag dient zur Freigabe der Verbindung und zeigt an, dass keine Daten mehr vom Sender kommen. Die FIN- und SYN-Flags haben Sequenznummern, damit diese in der richtigen Reihenfolge abgearbeitet werden.
Window	Ist die Anzahl der Daten-Oktetts (Bytes), beginnend bei dem durch das Acknowledgmentfeld indizierten Daten-Oktett, die der Sender dieses TCP-Paketes bereit ist zu empfangen.
Checksum	Die Prüfsumme dient zur Erkennung von Übertragungsfehlern und wird über den TCP-Header, die Daten und einem Pseudo-Header berechnet. Dieser Header besteht aus der Ziel-IP, der Quell-IP, der TCP-Protokollkennung (0x0006) und der Länge des TCP-Headers inkl. Nutzdaten (in Bytes).
Urgent Pointer	Zusammen mit der Sequenz-Nummer gibt dieser Wert die genaue Position der Urgent-Daten im Datenstrom an. Der Wert ist nur gültig, wenn das URG-Flag gesetzt ist.
Options	Das Options-Feld ist unterschiedlich groß und enthält Zusatzinformationen. Die Optionen müssen ein Vielfaches von 32 Bit lang sein. Sind sie das nicht, muss mit Null-Bits aufgefüllt

	werden (Padding). Dieses Feld ermöglicht, Verbindungsdaten auszuhandeln, die nicht im TCP-Header enthalten sind, wie zum Beispiel die Maximalgröße des Nutzdatenfeldes.

Quelle: Wikipedia

6.1.3 TCP-Verbindungsaufbau „3-Way-Handshake“

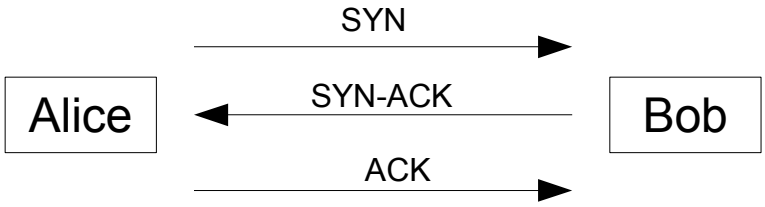


Abbildung 1: 3-Way-Handshake

Mit dem 3-Way-Handshake wird in Peer-to-Peer Netzwerken eine Verbindung zwischen zwei Punkten aufgebaut. Dabei wird die Verbindung formell ausgehandelt.

- **SYN** synchronize Alice will mit Bob sprechen.
- **SNY-ACK** synchronize acknowledge Bob sagt, dass das OK ist.
- **ACK** acknowledge Alice sagt, dass sie es verstanden hat.

6.2 Zustände von TCP

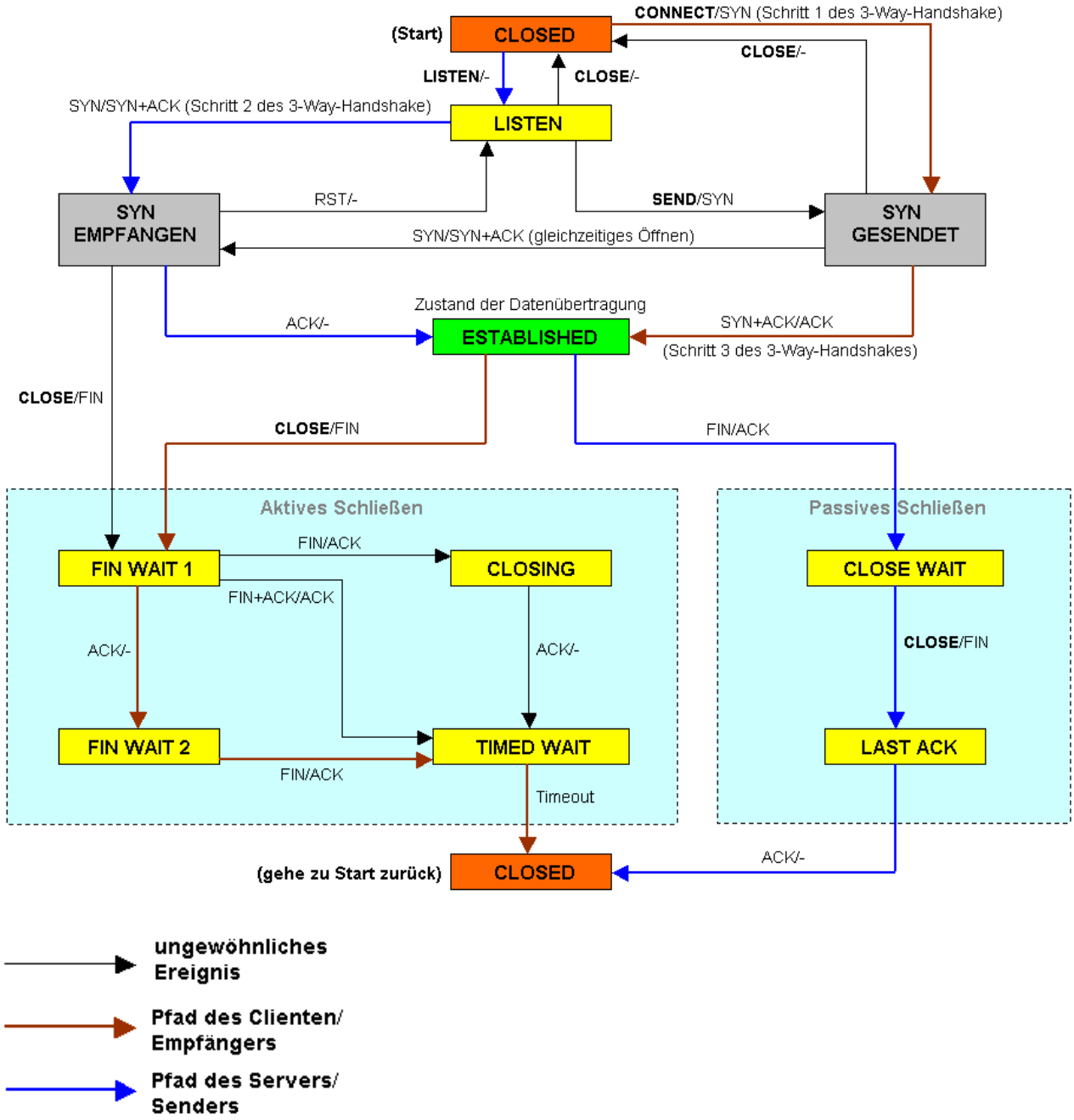


Abbildung 2: TCP Zustandsdiagramm

Quelle: http://upload.wikimedia.org/wikipedia/de/b/ba/Tcp_verbindung.png

6.3 Die SYN-Flood Attacke

Die SYN-Flood Attacke ist eine Denial of Service Attacke. Dabei wird der Verbindungsaufbau des TCP-Transportprotokolls verwendet. Bei erfolgreicher Attacke sind Dienste oder ganze Computer in einem Netzwerk nicht mehr erreichbar. DOS-Attacken haben das Ziel, das Zielsystem zu überlasten.

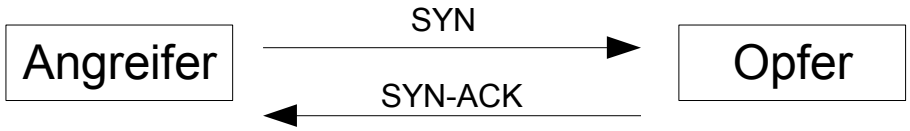


Abbildung 3: SYN-Flood Attacke

Bei der SYN-Flood-Attacke wird die ACK-Nachricht nicht gesendet. Das Opfer wartet auf die Antwort vom Angreifer. Die Verbindung ist noch halb offen, also noch nicht ganz abgeschlossen. Der Speicherbereich im Netzwerkstack bleibt aber weiterhin reserviert. Wenn man sehr viele Verbindungsanfragen stellt, ohne diese zu bestätigen überläuft schlussendlich der Speicher vom Opfer.

Als Gegenmassnahme können SYN-Cookies oder Firewalls dienen.

6.4 UDP – User Datagramm Protocol

6.5 Eigenschaften

- Verbindungslos
  - Kein Verbindungsaufbau zwischen den Partnern
- Unzuverlässig
  - Keine Sequenznummerierung und keine Bestätigung (Kommunikationsfehler / Zuverlässigkeit werden meistens durch die Anwendungsschicht geregelt)
- Identifizierung der Anwendungsschichtprotokolle
- Leichtes Protokoll
  - Schont Speicher (gut für DNS-Traffic)
- Mehrere Partner
  - Multicast, Broadcast / Streaming

6.5.1 UDP-Header

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source Port																Destination Port															
Length																Checksum															
Data																															

Felder

Feldinhalt	Bit	Beschreibung
Quell-Port (Source-Port)	16	Hier steht der Quell-Port, von der die Anwendung das UDP-Paket verschickt. Bei einer Stellenanzahl von 16 Bit beträgt der höchste Port 65535.
Ziel-Port (Destination-Port)	16	Hier steht der Ziel-Port, über welchen das UDP-Paket der Anwendung zugestellt wird. Bei einer Stellenanzahl von 16 Bit beträgt der höchste Port 65'535.
Länge	16	In diesem Feld wird angegeben, wie lang das gesamte UDP-Paket ist. Über diesen Wert kann die Vollständigkeit des UDP-Paketes ermittelt werden.
Check-Summe	16	Über dieses Feld wird kontrolliert, ob das UDP-Paket fehlerfrei übertragen wurde. Die Check-Summe bietet keinen Schutz vor Datenverlust.

Im Gegensatz zu TCP fehlen folgende wichtigen Felder: ACK-Nummer, SEQ-Nr

6.6 Unterschiede zwischen TCP und UDP

Eigenschaft	TCP	UDP
Aufbau des Headers	Umfangreich ACK-Nr; SEQ-Nr.	Einfach
Verbindungsaufbau	Formell	Nicht formell
Verbindungsverfahren	Verbindungsorientiert	Verbindungslos
Anwendungsprotokolle	SMTP, POP3, Telnet, FTP, ...	DNS, RDP, DHCP
Typisch für die Anwendungsprotokolle	Ziel muss im Moment des Verbindungsaufbaus erreichbar sein.	Ziel muss im Moment des Verbindungsaufbaus nicht erreichbar sein.
Besondere Kommunikationsart	Kein Streaming	Streaming

7 ICMP - Internet Control Message Protocol

7.1 Eigenschaften

- Zusatzprotokoll zu IP
- Diagnosemeldungen erzeugen
- Fehlerbenachrichtigung

7.2 ISO/OSI-Modell

- Layer 7: ping, tracert
- Keine Layer 4 Protokolle!!!
- Layer3: IP + ICMP

7.3 ICMP-Nachricht

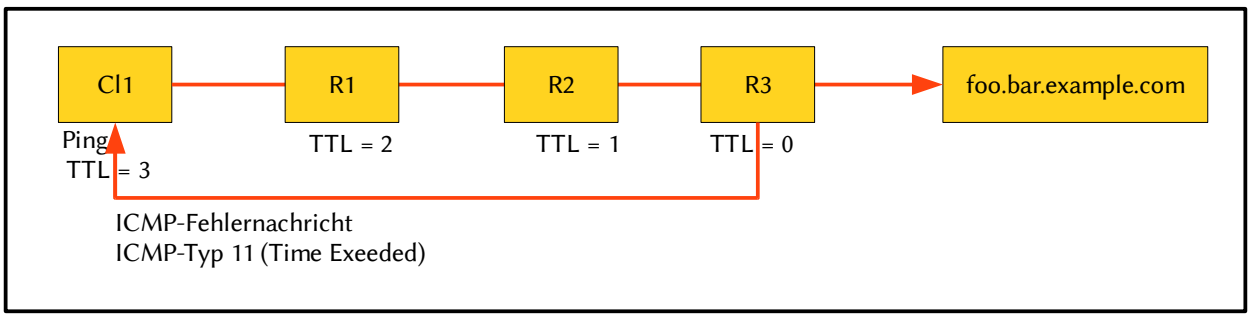
Ethernet	**IP** Protocol: 1	**ICMP** Type = xxx Code = xxx Checksum = xxx	Daten (optional)

Beispiel

```
⊞ Frame 154 (70 bytes on wire, 70 bytes captured)
⊞ Ethernet II, Src: ZyxelCom_4f:9d:df (00:19:cb:4f:9d:
⊞ Internet Protocol, Src: 4.69.134.117 (4.69.134.117),
⊟ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
  ⊞ Internet Protocol, Src: 10.11.2.160 (10.11.2.160),
  ⊟ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0 ()
      Checksum: 0xa1ff [correct]
      Identifier: 0x0200
      Sequence number: 21504 (0x5400)
```

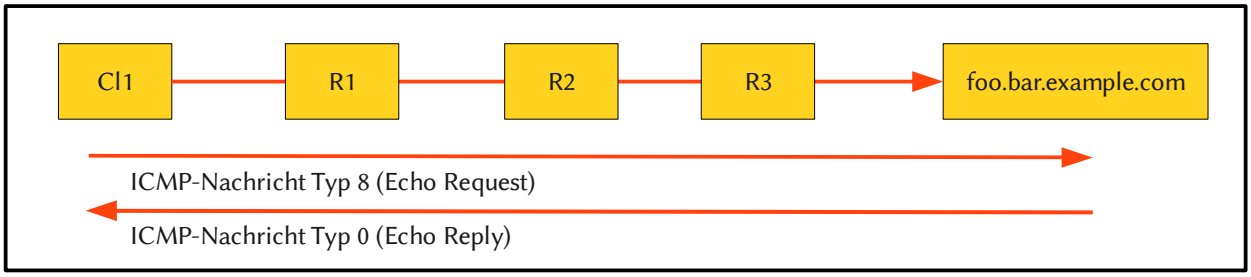
7.4 Beispielszenarien

ICMP Typ 11: Zeitlimit überschritten

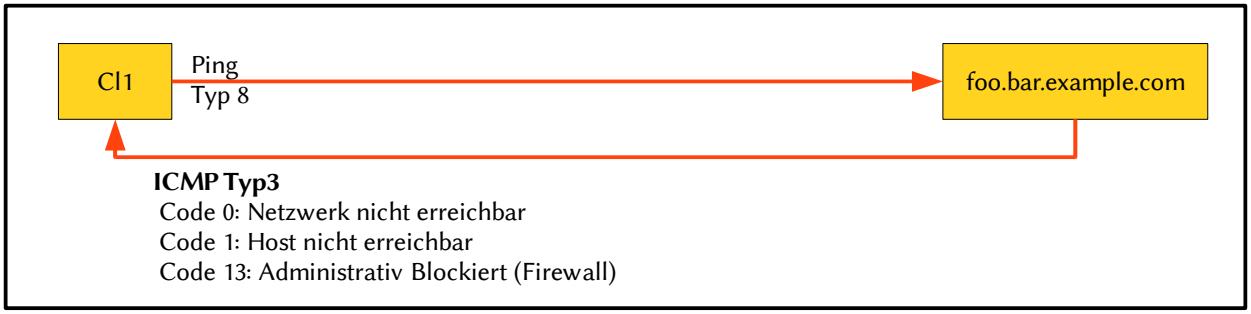


TTL wird herunter gezählt, damit das Internet nicht versauft, bzw. Pakete unendlich im Kreis tanzen.

ICMP Type 8 und 0: Echo Request und Echo Reply



ICMP Typ 3: Destination unreachable



7.5 ICMP-Typen und Codes

Typ	Typname	Code	Bedeutung
0	Echo-Antwort	0	Echo-Antwort
3	Ziel nicht erreichbar	0	Netzwerk nicht erreichbar
		1	Host (Zielstation) nicht erreichbar
		2	Protokoll nicht erreichbar
		3	Port nicht erreichbar
		4	Fragmentierung nötig, **D**on't **F**ragment aber gesetzt
		5	Route nicht möglich (die Richtung in IP-Header-Feld Option falsch angegeben)
		13	communication administratively prohibited (Packet wird von der Firewall des Empfängers geblockt)
4	Entlasten der Quelle	0	Datagramm verworfen, da Warteschlange voll
8	Echo-Anfrage	0	Echo-Anfrage (besser bekannt als „Ping“)
11	Zeitlimit überschritten	0	TTL (Time To Live, Lebensdauer) abgelaufen
		1	Zeitlimit während der Defragmentierung überschritten
30	Traceroute		Traceroute

Quelle: http://de.wikipedia.org/wiki/Internet_Control_Message_Protocol

8 Routing

8.1 Routing-Tabelle

Folgendermassen ist eine Routing-Tabelle aufgebaut:

Subnetzadresse	Subnetmaske	Next-Hop
Wie heisst die Adresse vom Subnet	Wie heisst die Subnetmaske?	Wohin muss ich das Paket weiterleiten?

```
emanuel@discordia:~$ route
Kernel-IP-Routentabelle
Ziel            Router          Genmask         Flags Metric Ref    Use Iface
link-local      *               255.255.0.0     U     1000   0        0 wlan0
10.0.0.0        *               255.0.0.0       U     0      0        0 wlan0
default         10.0.0.1        0.0.0.0         UG    0      0        0 wlan0
```

Router kommunizieren mit Routingprotokollen untereinander und handeln einen optimalen Weg aus.

8.1.1 Default Gateway

Der Default-Gateway wird genutzt, wenn wir aus dem aktuellen Subnetz ein Paket senden wollen. Der Host merkt, dass das Ziel nicht im selben Subnetz liegt und sendet deshalb das Paket an den Default-Gateway. Dies ist ein Router, welcher das Paket in das richtige Subnetz weiterleitet.

8.2 Routing-Tabelle bestimmen

- Alle Subnetze aufschreiben
- Die dazugehörige Subnetzmaske notieren. (Classful und Classless beachten!)
- Über welchen Router in meinem Netz ist das Subnetz „angeschlossen“. Das Interface von diesem Router auf „meiner Seite“ hinschreiben.

8.3 IP-Pakete weiterleiten

- Man nimmt die Destination IP-Adresse.
- Diese wird mit der ersten Subnetzmaske der Routing-Tabelle übereinandergelegt.
- Anhand der Subnetzmaske der Routing-Tabelle errechnen oder „erlugen aus der Tabelle“ die Subnetzadresse.
- Stimmt diese Subnetzadresse mit der Subnetzadresse der Routing-Table überein, kann diese passen.
    - Es kann jedoch sein, dass noch eine weitere Route übereinstimmt. Deshalb gehen wir ALLE EINTRÄGE der Tabelle durch!
    - Wenn mehrere übereinanderstimmen, nimmt man die „more specific“ bzw. eifach die „grössere“ Subnetzadresse (mit der kleineren Blockgrösse).

(Das gibt weniger Broadcast :D – oh ja – schön.)

- Wenn quasi keine übereinanderstimmt, ausser 0.0.0.0, dann wird diese genommen. Diese stimmt immer und wird auch Default-Route genannt.
- Nun schauen wir beim passenden Eintrag, an welchen Next-Hop das IP-Paket weitergeleitet werden soll. Dies machen wir auch so.

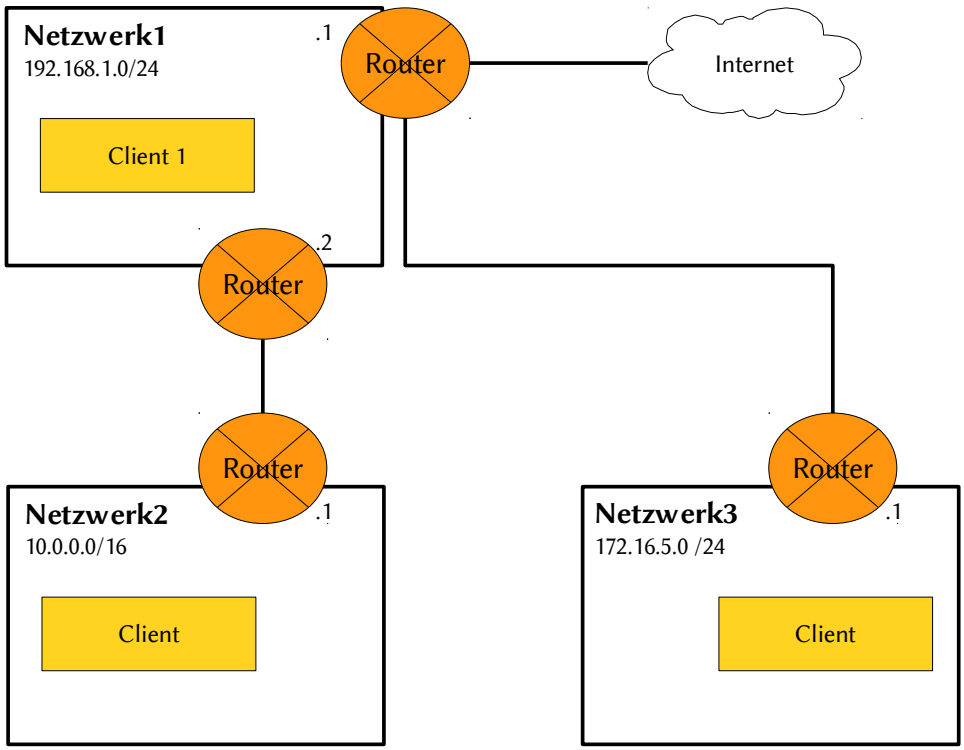
Kurz gesagt: Netzwerkadresse erstellen und vergleichen. Wenns passt, nimmt man den Next-Hop beim Eintrag mit der „grössten“ Subnetzmaske.

8.4 Routingtabellen interpretieren

Kurz und knapp zum Zeichnen des Netzes anhand der Routing-Tabelle:

- Man zeichnet zuerst den Host auf mit allen Interfaces (Schnittstellen).
- Dann macht man jeweils das Netzwerkziel an das entsprechende Interface dran.

8.5 Beispiel



Die Default-Route beim Client 1 ist bereits eingetragen, damit dieser ins Internet und ins Netzwerk 3 kommt.

Route für das Netzwerk 2 hinzufügen (Windows-Syntax)

```
route add 10.0.0.0 mask 255.255.0.0 192.168.1.2
```

Linux-Syntax:

```
route add -net 10.0.0.0 netmask 255.255.255.0 gw 192.168.1.2
```

9 PPP - Point-to-Point Protocol

9.1 Eigenschaften

- Standard für Punkt-zu-Punkt Verbindung
- Verkapselung der Datenverbindungsschicht; mehrere Protokolle gleichzeitig auf einer einzigen Verbindung
- Link Control Protocol (LCP) handelt die Datenverbindungsschichtparameter aus
- Network Control Protocol (NCP) handeln die Netzwerkschichtparameter aus

9.2 Anwendung

Anbindung von Netzwerken über xDSL an das Internet (Der Vorgang ist für die Benutzer transparent, die Auth.-Daten liegen beim Kunden auf dem PPP-Tunnelende (Public IP-adressierter Router).

Ein super gutes Prototokoll (Gellen Sie, Herr Gasser! ^^). <-- An der LAP nicht hinschreiben!!! ;-)

9.3 PPP Verbindungsaufbau

Es gibt vier Phasen; erst danach können Daten übertragen werden.

1. PPP-Konfiguration mit LCP: Verbindungsparameter werden konfiguriert.
2. Authentifizierung mit einem PPP-Authentifizierungsprotokoll, welches in Phase 1 ausgehandelt wurde (z. B. CHAP)
3. Rückruf: Wenn Authentifizierung erfolgreich: Antwortende PPP-Partner beendet Verbindung und baut eine Verbindugn zum PPP-Partner auf, der ursprünglich angerufen hat (Windows: Callback Control Protocol, CBCP)
4. Protokollkonfiguration mit NCPs: Individuelle Datenprotokolle und Hilfsdienste konfigurieren (Verschlüsselung, Komprimierung)

Übertragene IP-Konfiguration

- IP-Adresse (WAN-Seitig)
- Default Gateway
- Max 2 IP-Addr für DNS-Server
- Keine Subnetzmaske (da 255.255.255.255)!

9.4 Authentifizierungsprotokolle von PPP

9.4.1 CHAP (Challenge Handshake Authentication Protocol)

- RFC 1994
- Sicherer als PAP
- Normale Providerverbindung über Modem / Telefon
- Gut: Kennwort wird nicht übertragen
- Gut: Sichere Übertragung der Authentifizierungsdaten über das Netzwerk.
- Schlecht: Keine gegenseitige Authentifizierung (Nur der Client authentifiziert; keine Gewähr auf richtigen Server)

Schritte

1. Ein Client initiiert eine Verbindung zu einem Einwahlserver, und dieser verlangt eine Authentifizierung mittels CHAP. Dabei wird ein zufälliger Wert (die Challenge bestehend aus CHAP-Sitzungs-ID, Challenge-String und Benutzername vom Partner) an den Client übertragen, der sich authentifizieren muss.
2. Der Client bildet aus der Zufallszahl und dem Passwort einen Hashwert mittels einer one-way Hash-Funktion (zum Beispiel MD5) und überträgt diesen an den Einwahlserver. Unter der Annahme, dass die verwendete Hashfunktion eine Einwegfunktion ist, lässt sich das Passwort nicht wieder errechnen.
3. Der Einwahlserver errechnet ebenfalls einen Hashwert aus der Zufallszahl und dem bei ihm (im Klartext) hinterlegten Passwort. Wenn dieser mit dem vom zu authentifizierenden Rechner gesendeten Wert übereinstimmt, ist die Authentifizierung erfolgreich.

Quelle: http://de.wikipedia.org/wiki/Challenge_Handshake_Authentication_Protocol

Danach wird die IP-Konfiguration übergeben

9.4.2 PAP

Bei PAP wird das Passwort für die Authentifizierung unverschlüsselt zusammen mit der Benutzerkennung übertragen. Es ist damit durch passives Mithören ausspähbar. Dieser unsicheren Möglichkeit steht das komplexere Protokoll CHAP gegenüber. Bei dieser Methode wird durch Verschlüsselung und Entschlüsselung einer Zufallszahl der Zugang geprüft.

Quelle: http://de.wikipedia.org/wiki/Password_Authentication_Protocol

9.4.3 EAP

EAP ist ein Authentifizierungs-Protokoll, das unterschiedliche Authentisierungsverfahren (wie z. B. Username/Password (RADIUS), elektronische Zertifizierung, SIM (Subscriber Identity Module), etc.) unterstützt. EAP wird oft für die Zugriffskontrolle bei WLAN (Wireless Local Area Network)-Netzwerken genutzt.

EAP wurde entwickelt, um eine generische Unterstützung bei der Authentifikation, d. h. der Ein-

wahl, in ein fremdes Netzwerk zu schaffen, ohne dass man sich bei jeder neuen Authentisierung um die Infrastruktur kümmern und sie aktualisieren müsste. EAP ist heute weit verbreitet und wird von unterschiedlichen Transport-Protokollen, wie z. B. PPP (Point-to-Point Protocol), RADIUS (Remote Authentication Dial-In User Service) (RFC 2869), Diameter, unterstützt. Der IEEE 802.1X Standard schlägt u.a. EAP als Authentisierungsverfahren vor. Ebenso hat 3GPP den EAP-Standard zur Zusammenführung der GSM- mit der IP-Technologie übernommen. EAP könnte in Zukunft zudem zum bevorzugten Authentisierungsverfahren bei der WiMAX-Authentisierung werden.

Quelle: http://de.wikipedia.org/wiki/Extensible_Authentication_Protocol

9.4.4 PEAP

Das PEAP-Protokoll (Protected EAP) ist ein erweitertes EAP-Protokoll, das von Cisco und Microsoft entwickelt wurde. Bei diesem erfolgt der Verbindungsaufbau über das TLS-Protokoll, bevor das EAP-Protokoll für die Authentifizierung benutzt wird. In dieser Konstellation sind die Identifikationsdaten der Kommunikationspartner geschützt.

Quelle: www.itwissen.info

9.5 PPP-Frame

1 Byte	1 Byte	1 Byte	1 oder 2 Byte	Variabel	2 oder 4 Byte	1 Byte
Flag	Adresse	Steuerung	Protokoll	Nutzdaten / Payload...	Prüfsumme	Flag

Protokoll

Gibt den Code für die Paketart im Feld Nutzdaten an. Über LCP kann auch vereinbart werden, dass das Feld Protokoll nur 1 Byte groß sein soll.

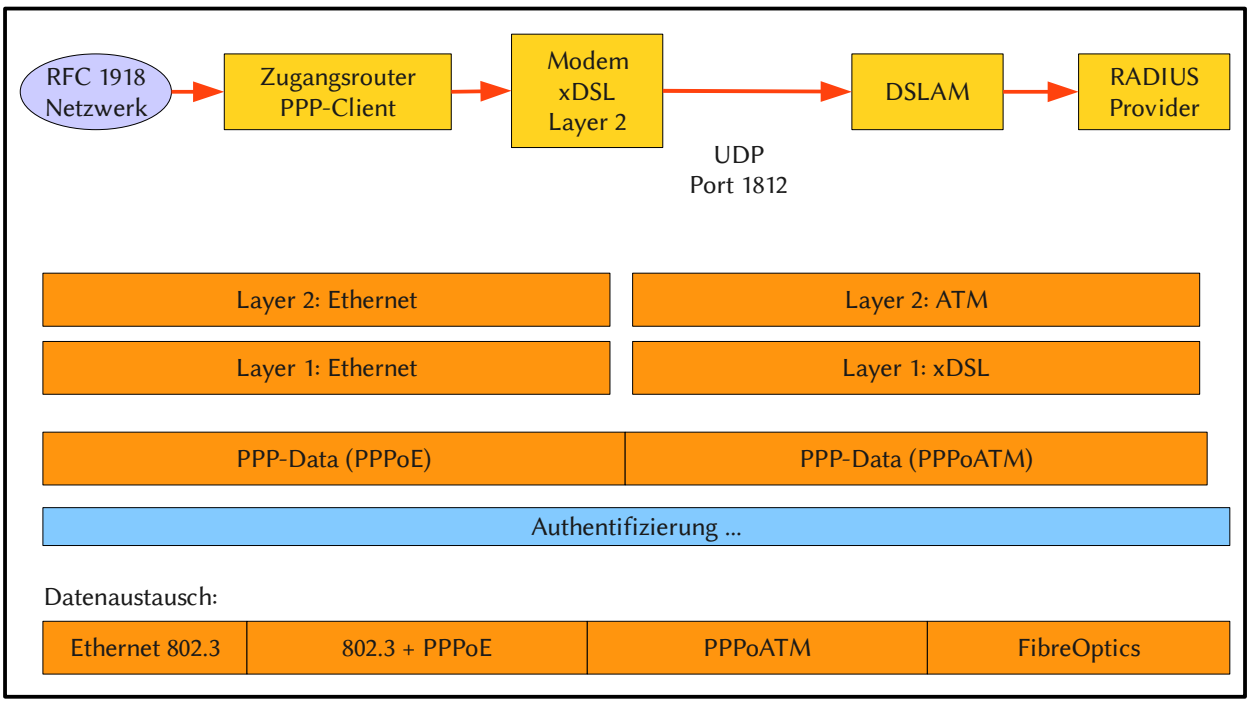
Hier eine Auswahl der Codes in hexadezimal:

- 0x0021 – Internet Protocol IP
- 0x80fd – Compression Control Protocol CCP
- 0x8021 – IP Control Protocol IPCP
- 0xc021 – Link Control Protocol LCP
- 0xc023 – Password Authentication Protocol PAP
- 0xc223 – Challenge Handshake Authentication Protocol CHAP

Nutzdaten

Das Feld Nutzdaten hat eine variable Länge, die durch LCP vereinbart wird. Dieses Feld kann bei Bedarf aufgefüllt werden (Padding).

9.6 PPP-Authentifizierung über eine xDSL-Strecke



DSLAM: Digital Subscriber Line Access Multiplexer

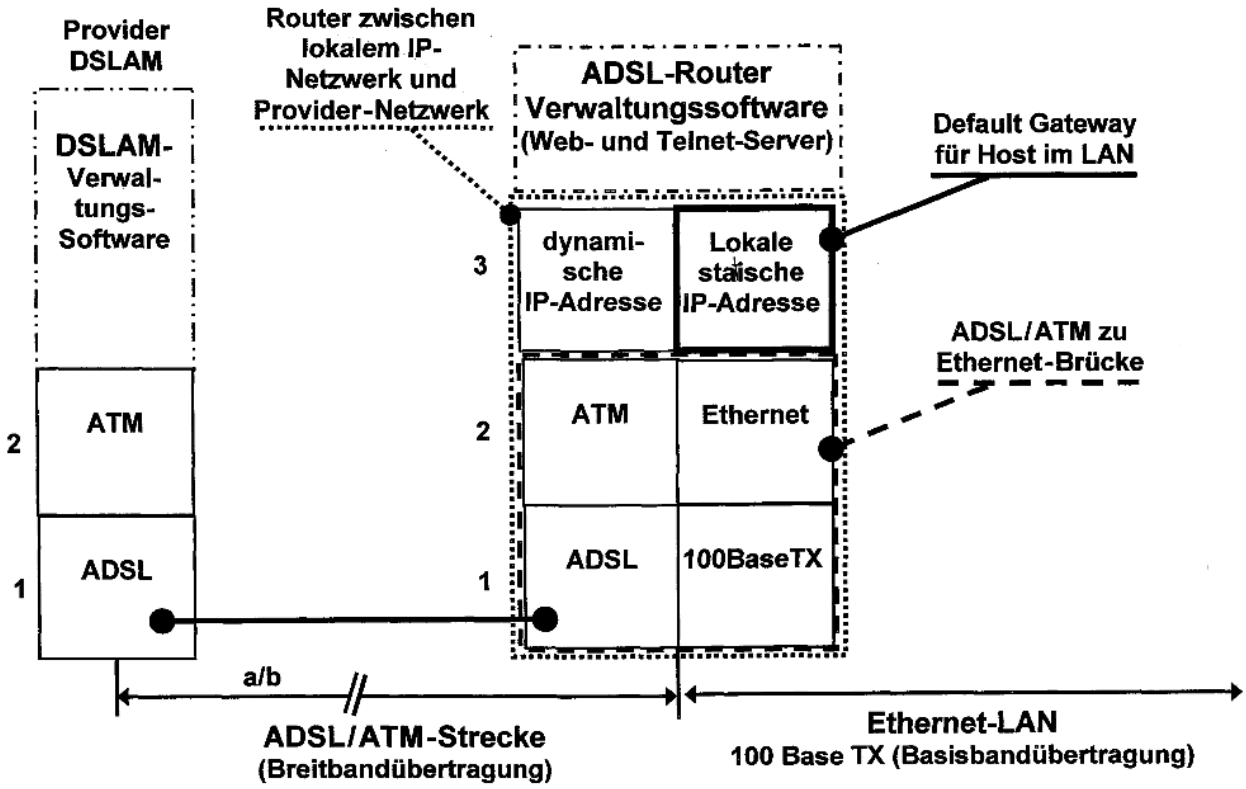
PPPoE-Frame

Ethernet	PPPoE	PPP	IP	UDP, TCP, ESP, ICMP	Nutzlast

PPPoATM-Frame

ATM	PPPoATM	PPP	IP	UDP, TCP, ESP, ICMP	Nutzlast

9.6.1 Layer-Darstellung



10 SNMP

SNMP bedeutet Simple Network Management Protocol.

10.1 Einsatzzwecke

1. Abfrage von Konfigurations-Einstellungen, Betriebs- und Leistungsparametern von Netzwerkgeräten.
2. Setzen von Konfigurationseinstellungen auf ein Netzwerkgerät (z.B. Ethernet-Port ein- oder ausschalten)
3. SNMP-fähige Geräte können Meldungen beim Auftreten eines bestimmten Ereignisses aussenden.

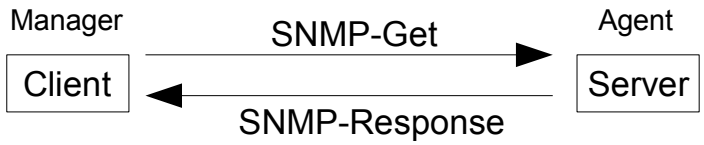
10.1.1 Einsatz von SNMP zur Überwachung von Applikationen

SNMP kann nicht nur zur Überwachung von Netzwerkgeräten dienen, sondern auch zur Überwachung von Applikationen. Beispiele sind folgende Applikationen.

- Cisco IOS
- Microsoft Exchange Server
  - Anzahl Nachrichten pro Minuten, Maximalgrösse, Dateigrössen, u.s.w...
- Microsoft SQL-Server
- Microsoft ISA-Server

Die MIB wird dabei um eigene OIDs ergänzt!

10.1 Client-Server Architektur von SNMP



Agent	Softwareprogramm, welches die Bearbeitung der Datenanforderung eines Managers übernimmt. Nach der Datenaufforderung eines Managers, kann der Agent die Daten eines verwalteten Objektes abrufen. Der Agent sendet auch so genannte Traps aus.
Manager	Softwareprogramm , welches Daten von einem Agenten im Netzwerk fordern kann. Der Manager verfügt üblicherweise über ein User- Interface, über den der Status und die abgerufenen Daten eines Host angezeigt werden können. Die Meldunge können auch archiviert werden.

10.2 MIB für SNMP

Definition von MIB (Management Information Base): Datendatei in der die Daten der verwalteten Objekte eines Host gespeichert sind. Jeder Host kann über mehrere MIBs verfügen.

SNMP wird typischerweise in heterogenen Umgebungen eingesetzt. Es werden also unterschiedliche Betriebssysteme eingesetzt.

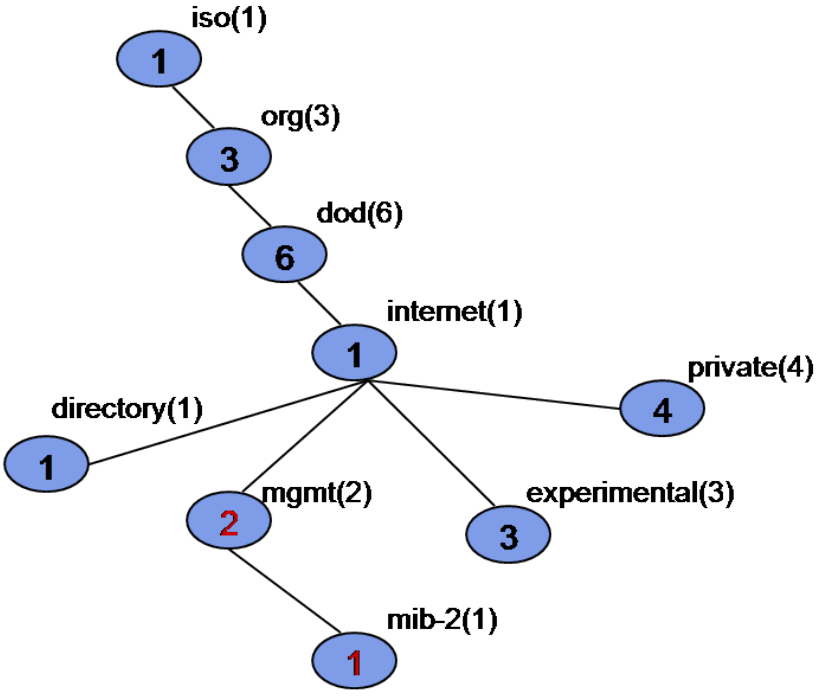
Daher müssen die SNMP-Informationen in einer platformübergreifenden Ordnungsstruktur abgelegt werden. Diese Informationsstruktur wird von der IANA verwaltet und ist in RFCs geschrieben:

Was	RFC-Nr	Beschreibung
MIB	1212	Concise MIB Definitions
MIB-II	1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
SNMP	1157	SNMP- Kommunikationsformate und Abläufe

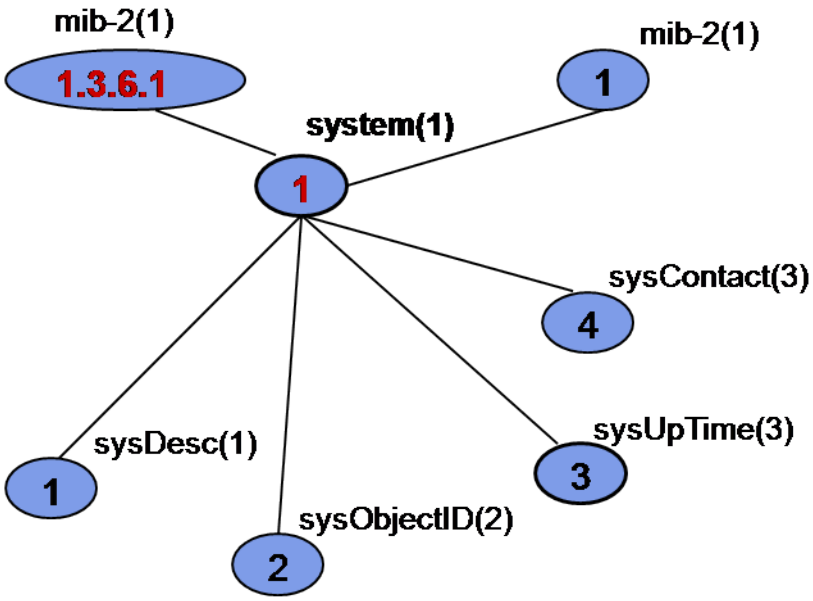
10.2.1 Object Identifier Trees (OID)

Die **einzelnen Informationsinhalte** der MIB werden als Objekte bezeichnet. Die Objekte werden in einer baumartig aufgebauten Hierarchie abgelegt. Durch diese Art der Gliederung wird das Informationssystem praktisch unendlich **erweiterbar**. Die einzelnen Informationen tragen Nummern.
Diese MIB-Objektnummern werden als OID (Object-Identifier) bezeichnet.

Die IANA definiert nicht nur die OIDs für SNMP, sondern auch die für LDAP, das z.B: von Active-Directory verwendet wird. LDAP ist im „directory“-Baum zu finden.



10.2.2 Unterbereiche von MIB-2



Mit einem sogenannten MIB-Browser kann die MIB eines Gerätes mit aktiviertem SNMP-Agenten durchforstet werden, ohne eine SNMP-Management Software zu installieren.

Unterbereich System

Unter dem System-Ast sind folgende Einträge zu finden:

MIB-2-Bezeichnung	MIB-2-OID	Beschreibung
sysDescr	.1.3.6.1.2.1.1.1	Hardwaretyp, Betriebssystem, Netzwerksoftware
sysObjectID	.1.3.6.1.2.1.1.2	Herstellerabhängige ID
sysUpTime	.1.3.6.1.2.1.1.3	Wie lange das System schon läuft
sysContact	.1.3.6.1.2.1.1.4	Welche Person man bei Fragen kontaktieren soll.
sysName	.1.3.6.1.2.1.1.5	Name vom Gerät. Oft wird die FQDN gewählt
sysLocation	.1.3.6.1.2.1.1.6	Wo befindet sich das Gerät physikalisch.
sysServices	.1.3.6.1.2.1.1.7	Was ist die Hauptaufgabe von diesem System. Diese Informationen sind nach dem OSI-Modell gespeichert.

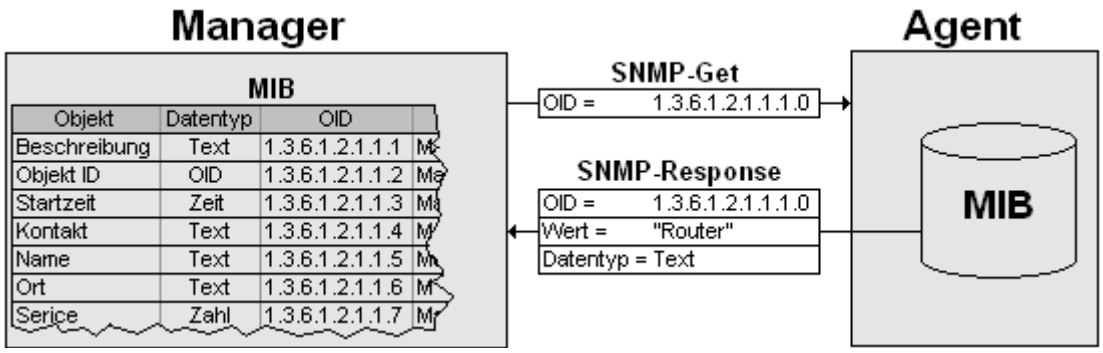
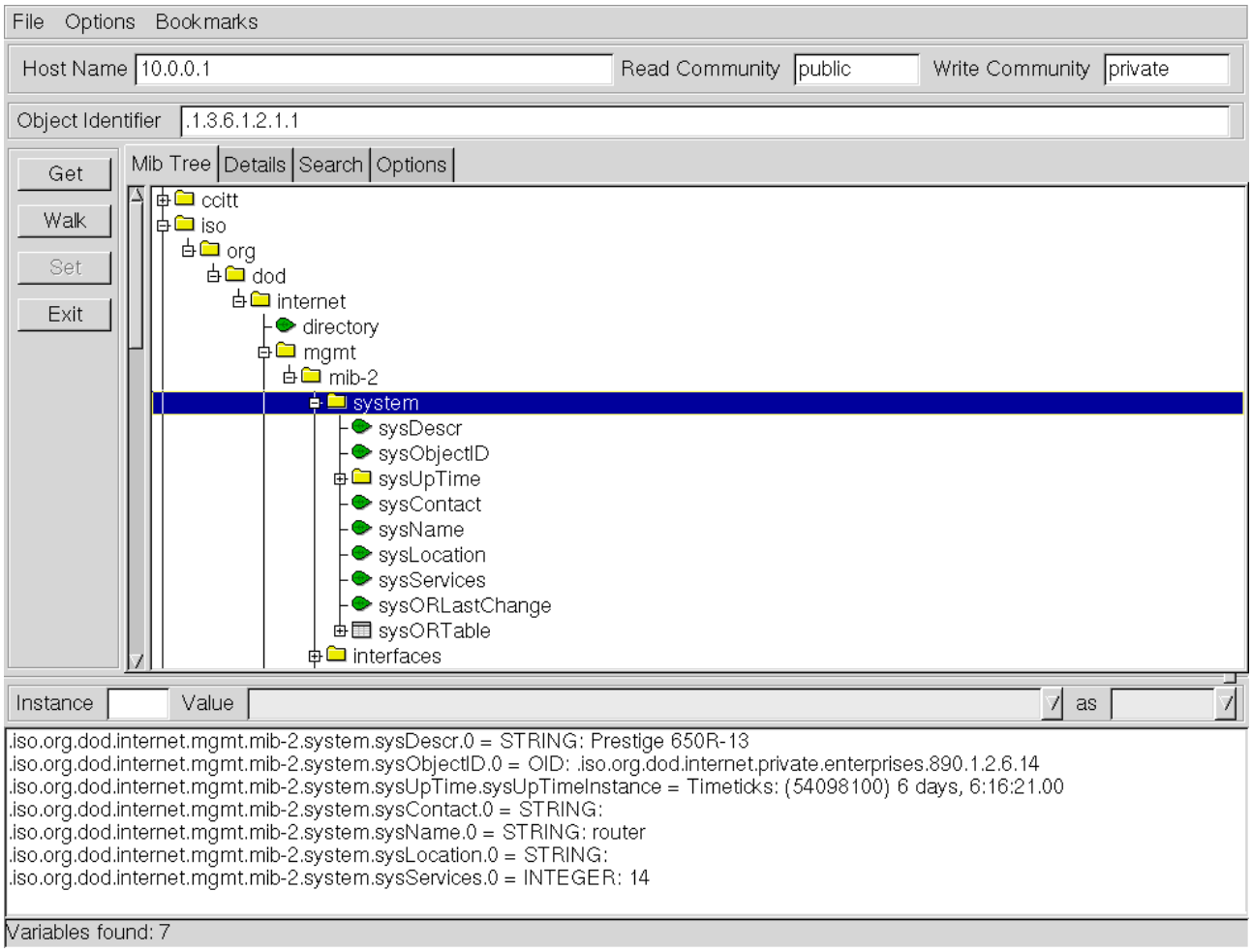


Abbildung 4: Quelle Bild: Wikipedia

10.3 Ein SNMP-Browser: mbrowse



Wir sehen den Ast.1.3.6.1.2.1.1. Im Unteren Teil sehen wir die Ergebnisse von meinem Heimrouter:

```
SNMPv2-MIB::sysDescr.0 = STRING: Prestige 650R-13
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-
SMI::enterprises.890.1.2.6.14
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (54118600) 6
days, 6:19:46.00
SNMPv2-MIB::sysContact.0 = STRING:
```

```
SNMPv2-MIB::sysName.0 = STRING: router
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 14
```

10.4 Aufbau des Ethernet-Rahmens

<table>
<tr>
<td>Ether

SRC-MAC: Unicast
DST-MAC: Unicast
Ether-Type:0x0800 (IP)</td>
<td>IP
Scr-IP: Unicast
Dst-IP: Unicast
Protocol: 0x11 (UDP)</td>
<td>UDP
Src-Port
Dst-Port:161</td>
<td>SNMP
Community: public
PDUType: GET</td>
</tr>
</table>

Capture-Filter, damit man nur SNMP-Pakete hören kann: „snmp“ oder „udp port 161“.

Ports

- SNMP: 161/UDP
- SNMP-Trap: 162/UDP

10.5 SNMP-Datagramme

PDU-Type = Protocol Data Units

PDU-Type	Aka	Beschreibung
GetRequest	Get	Meist verwendeter PDU-Type. Fragt den Agent nach einer Information in der MIB.
GetNextRequest	GetNext	Nach dem der Abfragecursor im MIB-Baum an einer bestimmten Stelle steht, soll die nächste Information nachgefragt werden.
GetResponse	Response	Eine simple Antwort auf ein Get, GetNext oder Set. Alle Anfragen werden so beantwortet.
SetRequest	Set	Eine in der MIB existierende Variable soll geändert werden. Man mus die richtigen Berechtigungen haben.
Trap		SNMP-Agenten können programmiert werden, dass diese bei einem bestimmten eintreffen eines Ereignisses einen Trap losschicken, um den Client mit Infos zu beliefern. Z.B. Bei einem Fehlerfall. Unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist.

10.6 SNMP-Sicherheit

- Dienen Zugriffsberechtigungen. Zugriffschschutz.
- dient jedoch nicht der Sicherheit!
- Zwei Standard-Communities: Public und Private
  - Public: Read Only

- Private: Read / Write

10.6.1 SNMP Community Strings

READ-ONLY	Get und GetNext kann gesendet werden, wenn der Agent der selbe String verwendet wie der Request.
READ-WRITE	Get und Set: Lesen und Schreiben.

11 IPSec (VPN)

VPN erklärt am Beispiel IPSec.

11.1 Allgemein

- IPSec ist eine Protokoll-Suite, die von mehreren RFCs beschrieben werden.
- IPSec stellt End-zu-End Verbindunge verschlüsselt her (nur die zwei beteiligten Endknoten wissen von einer Verschlüsselten Verbindung; die anderen Teilnehmer merken gar nichts)
- Die Netz zu Netz-Verbindung wird durch IPSec im Tunnelmodus ebenfalls übertragen.
  - Verbindet RFC 1918-Netzwerke über das Internet

11.2 Alternative zu IP-in-IP

Layer-3-Paket in Layer-3-Paket (IP-in-IP) zum Verbinden von zwei RFC 1918 Netzwerken

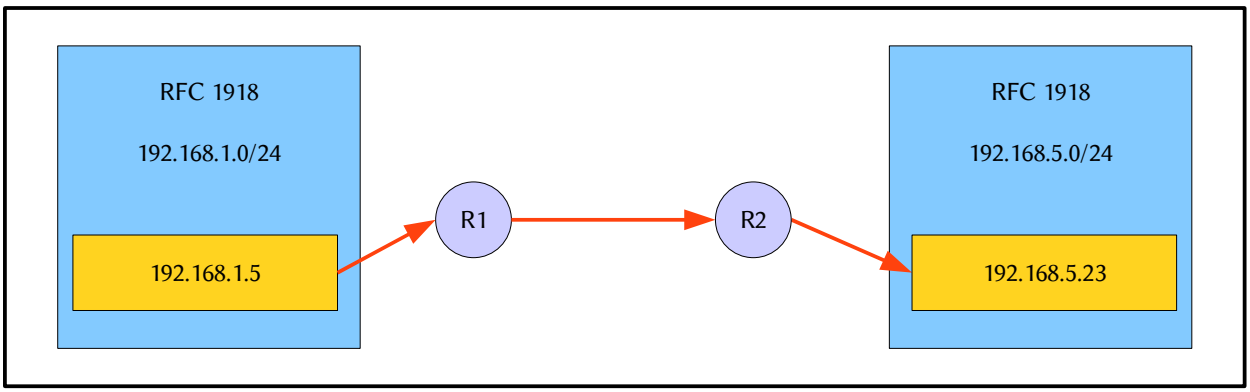


Abbildung 5: IP-in-IP

IP-Header DST: R2ext SRC: R1EXT	**IP-In-IP-Header** SRC: IP1 DST: IP2 Protokoll: 4 (IP-in-IP)	**TCP**

11.3 Leistung von IPSec

Gegenseitige Identifizierung der Tunnel-Endpunkte

Die ISAKMP-Software der Tunnelendpunkte überprüft gegenseitig die Identität. So wird vor der Versendung von Daten sichergestellt, dass die Daten nicht an einen gefälschten Tunnelendpunkt geleitet werden.

Als Autentifizierungsverfahren kommen folgende Verfahren in Frage:

- PSK (Pre Shared Key) (Schlüssel wurde im Voraus ausgetauscht)
- Kerberos

- privaten und öffentlichen Schlüsseln (Zertifikate; X509, PKI)

Vertraulichkeit der Daten

Die Daten werden verschlüsselt übertragen.

Als Verschlüsselungsverfahren kommen aus Performance-Gründen nur symmetrische Verfahren in Frage. Das bekannteste Verfahren ist 3DES („Triple DES).

Integrität der Daten

IPSec stellt sicher, dass die Daten auf ihrem Übertragungsweg nicht verändert werden können.

Eine Veränderung von Daten würde durch das eingesetzte Verfahren zur Sicherstellung der Datenintegrität (Hash-Bildung), erkannt.

Schlüsselverwaltung (Key Management)

IPSec hat mit ISAKMP ein aufwendiges Protokoll zum Aufbau und Verwaltung der symmetrischen Verschlüsselungs-Schlüssel implementiert.

Nach einer einstellbaren Datenmenge oder Übertragungsdauer wird automatisch ein neuer symmetrischer Verschlüsselungs-Schlüssel auf den Tunnelendpunkten erzeugt.

Der neue Verschlüsselungs-Schlüssel wird jeweils vollständig neu erzeugt, d.h. er hängt nicht vom vorhergehenden ab und wird auch nicht von diesem transportiert.

Merkmale

- Partnerauthentifizierung
  - Identität des Partners wird überprüft
  - PSK, Public-Key-Verfahren (X.509-Schlüssel) oder Kerberos
- Authentifizierung der Datenherkunft
  - Jedes Paket erhält eine Hash-Prüfsumme, mit der manipulierte Daten erkannt werden können.
- Datenintegrität
  - Ohne Schlüssel kann man die Prüfsumme nicht anpassen und somit kann man ohne Schlüssel keine Daten manipulieren
- Vertraulichkeit der Datenanforderung
  - Ohne Schlüssel sind die Daten nicht lesbar
- Wiederholungsschutz
  - Eine fortlaufende Nummer macht, dass man sich ein Angreifer nicht in eine Verbindung „einklinken“ kann (Man in the Middle-Attacke)
- Schlüsselverwaltung
  - Schlüssel werden sicher ermittelt und regelmässig geändert; nur Bruteforce würde hel-

fen

11.4 Algorithmen

Hashalgorithmen

- MD5 (Message Digest 5)
  - 128 Bit-Hashwert und 96-Bit-Schlüsselwert
- SHA1 (Secure Hash Algorithm 1) (Sicherer)
  - 160 Bit-Hashwert und 96-Bit-Schlüsselwert

Verschlüsselungsalgorithmen

- DES (Date Encryption Standard)
  - 56-Bit Schlüssel; 64-Bit-Datenblöcke
- 3DES (Triple DES)
  - Dreimal 56-Bit Schlüssel; Benötigt mehr Rechenzeit
- AES (Advanced Encryption Standard)
  - 128,192,256 Bit-Schlüssel

Diffie-Hellman-Schlüsselaustausch

Zwei Zahlen werden ausgetauscht und daraus der Schlüssel gebildet. Der Schlüsselaustausch geschieht unverschlüsselt und jeder kann mithören. Ein Mithörer kann jedoch den Schlüssel nicht nachbilden.

11.4.1 Übertragungsmodus

Quellen: http://www.virenschutz.info, http://de.wikipedia.org/wiki/IPsec

Tunnel-Mode

- Das zu übertragende IP-Datenpaket wird in ein weiteres IP-Datenpaket eingekapselt und verschlüsselt.
- Das eingekapselte IP-Datenpaket ist die Nutzlast vom übertragenen IP-Datenpaket.
- Die Quell- und Ziel-Adresse bleibt somit verborgen.
- Wird meist mit ESP genutzt.
- Es sind nur die Tunnel-Endpunkte mög-

Transport-Mode

- Es wird nur die eigentliche Nutzlast verschlüsselt.
- IP-Header bleibt unverändert.
- Die Quell- und Ziel-Adresse ist sichtbar.
- Die Verarbeitungsgeschwindigkeit ist schneller als beim Tunnel-Mode.
- Für interne Zwecke im LAN geeignet
- Wird meist mit AH genutzt.
- Für Host-zu-Host Verbindungen geeignet

lich

- Man kann ganze LANs verbinden

11.4.2 Sicherheitsprotokolle

Authentication Header (AH)

- Daten können von unbefugten ausgelesen werden, da keine Verschlüsselung.
- Es wird jedoch mittels einer Prüfsumme (Hash-Wert) geprüft, ob das Datenpaket während der Übertragung manipuliert wurde.
- Schutz vor wiederholten Senden von Paketen (Replay-Attacken)
- Der Authentifikations-Header befindet sich direkt vor den Nutzdaten.

Encapsulation-Security-Payload (ESP)

- Daten können von unbefugten nicht ausgelesen werden, da die Daten verschlüsselt werden.
- Es wird jedoch mittels einer Prüfsumme geprüft, ob das Datenpaket während der Übertragung manipuliert wurde.
- Schutz vor wiederholten Senden von Paketen (Replay-Attacken)
- Der IP-Header wird nicht überprüft. Deshalb ist es nur in internen Netzwerken zu verwenden.

11.4.3 Verbindungsaufbau

Um eine gesicherte Verbindung zwischen zwei Stationen aufbauen zu können, müssen auf beiden Seiten viele Parameter wie z.B. Art der gesicherten Übertragung (AH oder ESP), Verschlüsselungsalgorithmus, Schlüssel, Gültigkeit u.s.w ausgetauscht werden.

Main Mode

Der Verbindungsaufbau geschieht in 5 Schritten:

1. Senden von mehreren Vorschlägen mit Authentifizierung- und Verschlüsselungsalgorithmen.
2. Auswahl von der Gegenstelle des sichersten Algorithmus.
3. Senden des öffentlichen Schlüssels und einen zufälligen Wert.
4. Antwort der Gegenstelle mit ihrem öffentlichen Schlüssel und einem zufälligen Wert.
5. Authentifizierung über das jeweilige Verfahren (PSK oder Zertifikate).

- Sicherer, da verschlüsselt

Aggressive Mode

- Der Verbindungsaufbau wurde auf 3 Schritte gekürzt.
- Keine Verschlüsselung (Hashwert des PSKs wird im Klartext übertragen)
- Da in der Praxis oft schlechte Schlüssel gewählt werden, sollte man diesen Schlüssel vorsichtig verwenden.
- Hash-Werte werden im Klartext übertragen.
- Schneller
- Im Internen Netz verwendbar.

- Langsamer

11.4.4 Verschlüsselungsverfahren

PSK (Pre-Shared Key)

PSK (Pre-Shared Key) ist das symmetrische Verschlüsselungsverfahren. Hierbei müssen beide Teilnehmer den selben Schlüssel verwenden. Diese Methode ist einfach zu realisieren und schneller als die asymmetrische Methode. Das Problem liegt jedoch beim Schlüsselaustausch.

X.509-Zertifikat

Dieses Zertifikat ordnet ein Public-Key eindeutig seinem Inhaber zu. Für die Glaubwürdigkeit steht dessen Aussteller gerade, die CA (Certification Authority). Die CAcert-Zertifizierungsstelle vergibt kostenlos X.509-Zertifikate.

11.4.5 PFS - Perfect Forward Secrecy

- PFS verhindert, dass ein Angreifer dem es gelingt einen Schlüssel zu brechen, auch weitere Schlüssel einfach angreifen kann.
- Die Schlüssel werden in kurzen Abständen gewechselt und haben keinen Zusammenhang zueinander.
- Deutlich höherer Aufwand zur Generierung der Schlüssel (asymmetrische Verfahren).
- Bei den meisten Verschlüsselungsverfahren kann deshalb PFS deaktiviert werden.
- Folgende Protokolle verwenden PFS: IPSec, SSH, Off-the-Record Messaging

11.5 ISAKMP

Internet Security Association Key Management Protocol: P2P-Mässig, kein Client-Server-Konzept.

Läuft zwischen den IPSec-Tunnelendpunkten vor dem ESP-gekapselten Datenaustausch.

UDP-Port 500; Capture-Filter: udp port 500

Aufgaben von ISAKMP

1. Aushandlung des zu verwendenten Verschlüsselungsverfahren und darauf die gegenseitige Identifikation der Tunnel-Endpunkte.
2. Aushandlung der des Verschlüsselungs- und Hash-Algorithmus und dann der Aufbau eines gemeinsamen Verschlüsselungsschlüssels in aller Öffentlichkeit

Zwei Phasen

1. Hauptmodus
    1. Initiator sendet Vorschläge für Verfahren
        1. Authentifizierung

        1. Pre Shared Keys (PSK)
        2. Kerberos (mit Active Directory)
        3. Asymmetrische Verschlüsselung (PKI; Zertifikat)
    2. Symmetrisches Verschlüsselungsverfahren
        1. DES (Digital Encryption System, gilt heute als unsicher)
        2. 3DES („triple DES“, gilt heute noch als sicher)
        3. AES (Advanced Encryption Standard: gilt heute als Standard für Ipsec)
        4. Blowfish (gilt heute noch als sicher)
2. Der Responder wählt aus den angebotenen und den von ihm unterstützten Algorithmen den sichersten aus und sendet das Auswahlergebnis an den Initiator.
3. Der Initiator sendet seinen öffentlichen Teil vom Diffie-Hellman-Schlüsselaustausch und einen zufälligen Wert (Nonce).
4. Der Responder sendet ebenfalls seinen öffentlichen Teil vom Diffie-Hellman-Schlüsselaustausch und einen zufälligen Wert. Dieser Wert dient im Schritt 5 der Authentisierung.
    1. Diffie-Hellmann: Erzeugung eines geheimen Schlüssels zwischen zwei Partnern in aller Öffentlichkeit.
5. Schritt 5 ist die Authentisierung. Dabei müssen sich beide Beteiligten gegenseitig als zugriffsberechtigt ausweisen.

2. Schnellmodus (Periodische Schlüsselerneuerung, damit es sicherer ist)
    1. SA = Security Association --> Je einen symmetrischen Verschlüsselungsschlüssel für beide Übermittlungsrichtungen
        1. DES, 56 Bit, ist veraltet!!!
        2. 3DES (3x 56 Bit)
        3. AES (128,192,256 Bit)

ISAKMP Protokoll

<table>
<tr>
<td>IP

SRC: IPSecGW1
DST: IPSecGW2
Protocol = 17 (UDP)</td>
<td>
<table>
<tr>
<td>UDP

SRC-Port: 500
DST-Port: 500</td>
<td>
<table>
<tr>
<td>ISAKMP

Header...</td>
<td>Payload</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>

11.6 Tunnelmodus Datenübertragung

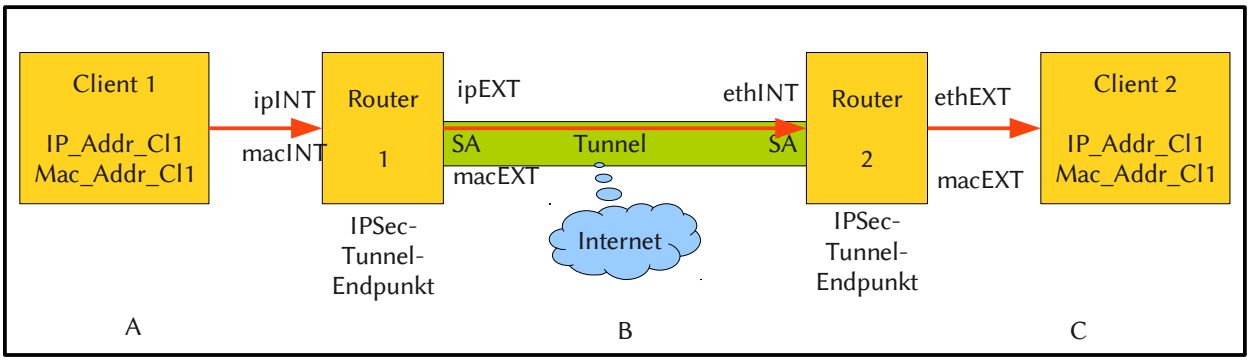


Abbildung 6: Tunnelmodus Datenübertragung

A: Client 1 – Router 1

Layer 2 Ethernet-Frame SRC-MAC: C1Mac DST-MAC: R1MacInt Type: 0x800 (IP)	**Layer 3 IP-Packet** SRC_IP: C1IP DST_IP: C2IP Protocol: 1 (ICMP)	**Layer 3+ ICMP** Type 8 (echo request; ping)	ping fnord.foo.local

Protocol: 50: ESP (IPSec) Filter: ip proto 50

B: Router 1 – Router 2

Layer 2 Ethernet-Frame / ATM SRC-MAC: R1Mac DST-MAC: UNKNOWN Type: IP (0x800 bei Ethernet)	**Layer 3 IP-Packet** SRC_IP: R1IP DST_IP: R2IP Protocol: 50 (ESP)	**Layer 3 ESP** Sequenz: Nr	**Layer 3 IP-Packet** SRC_IP: C1IP DST_IP: C2IP Protocol: 1 (ICMP)	**Layer 3+ ICMP** Type 8 (echo request; ping)	ping fnord.foo.local

11.6.1 IPSec NAT Traversal

Die IP-Addresse des Tunnelendpunktes wird im ISAKMP verwendet.

Wenn diese Adresse im IP-Header durch NAT getauscht wird, führt dies zu Problemen:

- NAT Traversal vermeiden!

Steht der IPSec-Gateway hinter einem NAT-Router, dann: #FAIL!!!

11.7 IPSec-Funktionen im Überblick

Funktion	Kategorie	Intern / Extern // Info
Tunnel-Mode	Übertragungsmodus	Extern, da Gesamtes IP-Paket verschlüsselt // LAN-LAN; Host-LAN, Host-Host
Transport Mode	Übertragungsmodus	Intern, da nur Nutzlast verschlüsselt // Nur Host-Host
AH	Sicherheitsprotokoll	Intern, da nicht verschlüsselt
ESP	Sicherheitsprotokoll	Extern, da verschlüsselt
Main Mode	Verbindungsaufbau	Extern, da verschlüsselt (dafür langsamer)
Aggressive Mode	Verbindungsaufbau	Intern, da nicht verschlüsselt (dafür schneller)
PSK	Verschlüsselungsverfahren	Intern, da nur ein Schlüssel // Symmetrisch (Schneller)
PKI	Verschlüsselungsverfahren	Extern, da besserer Überblick / Kontrolle // Asymmetrisch
PFS		Extern, da es sicherer ist und nur mit PKI verwendbar ist.

Tabelle 5: IPSec Funktionen im Überblick

12 VPN-Arten im Überblick

VPN-Art	Vorteile	Nachteile
IPSec	Zugriff nur von erlaubten Rechnern aus möglich Access Policies und unternehmensweite Sicherheitsrichtlinien (z.B. Virenschutz) wirksam Kompletter Zugriff auf Unternehmensressourcen und Anwendungen	Bindet Benutzer an bestimmte Rechner Erfordert umfangreichere Benutzerverwaltung Firewalls und NAT kann den Zugriff verhindern
OpenVPN	Sicher und einfach zu konfigurieren Port, Protokoll, etc. frei wählbar Hohe Kompatibilität mit Firewalls, Proxies, … Nur ein, frei wählbarer Port notwendig HTTPS – Jeder Proxy kann getunnelt werden Umfangreiche Scripting-Möglichkeiten Flexible Netzwerkkonfiguration High Performance Einfache Installation und Konfiguration Verfügbar für alle Plattformen	Da das Projekt OpenSource ist, können von Programmierern absichtlich Sicherheitslücken eingebaut werden. Diesen Vorfall hat es schon einmal gegeben.
PPTP	Verfügbarkeit - Da PPTP im Lieferumfang von Windows (ab NT) enthalten ist, ist es ohne Zusatzsoftware unmittelbar verfügbar. Simple Einrichtung. Diverse Protokolle nutzbar (IP, NetBEUI, IPX)	Defizite bei der Schlüsselverwaltung (Sicherheit) Nicht mehr sicher ohne Zertifikate
SSL-VPN	Vielfalt an Webbrowser ermöglicht fast universellen Zugriff Erlaubt dedizierten Zugriff auf Applikationsebene Einfacher Zugriff auf webbasierte Anwendungen In der Regel geringere Kosten (TCO) als IPSec Einfachere Skalierbarkeit	Zugriff von nicht gesicherten Rechnern möglich Token oder digitale Zertifikate werden benötigt um Angriffe auf das Passwort zu verhindern. Sensible Informationen können auf unsicheren Rechnern zurückgelassen werden Wenige Applikationen unterstützen out-of-the-box webbasierten Zugriff.
Hamachi	Verschlüsseltes Instant Messaging (AES-256) Sicherer Datei Tausch über virtuelles LAN Das Spielen von Games über virtuelles LAN!	Freigaben welche im LAN freigegeben wurden, werden automatisch auch im Hamachi Netzwerk freigegeben Zu unsicher für Geschäftsumfeld Langsamer, da es immer über einen Hamachi-Server geht.

13 VLAN (IEEE 802.1Q)

Auf einer physischen LAN-Verkabelung werden mehrere virtuelle LANS gebildet. Jedes VLAN hat eine eindeutige Nummer. Die Pakete mit der ID 222 werden nur an die Switch Ports ausgegeben, die sich im VLAN 222 befinden.

Trunk: bündel von mehreren VLANs. Es werden alle Inputs auf diesem Port ausgegeben. Ein Kabel für alle VLANs. Oft wird dies gemacht, um mehrere VLAN-Switches miteinander zu verbinden.

13.1 Vorteile

- Zuweisung von IP-Teiletzen auf Stufe Switch-Port und nicht für den ganzen Switch
- Verkleinerung der MAC-Broadcast-Domäne

13.2 VLAN-Typen

Port-Basiert	**Tag-Basiert**
Ein Switch wird in mehrere logische Switches segmentiert. Ein Port gehört immer nur zu einem VLAN.	Das ein- und austaggen geschieht auf den Switches.

Tabelle 6: VLAN-Typen

13.3 VLAN-Ethernet-Frame

Das Ethernet-Frame wird mit dem VLAN-Tag erweitert:

6 Bytes	6 Bytes	**VLAN-Tag (4 Bytes)**				2 Bytes	Bis 1500 Bytes	4 Bytes
		16 Bit	3 Bit	1 Bit	12 Bit			
DST-Mac	SRC-Mac	Protocol ID	User Priority	Connonical Format Indicator	VLAN ID	Type / Len	Data	Frame Check

13.4 VLAN (Layer 2)

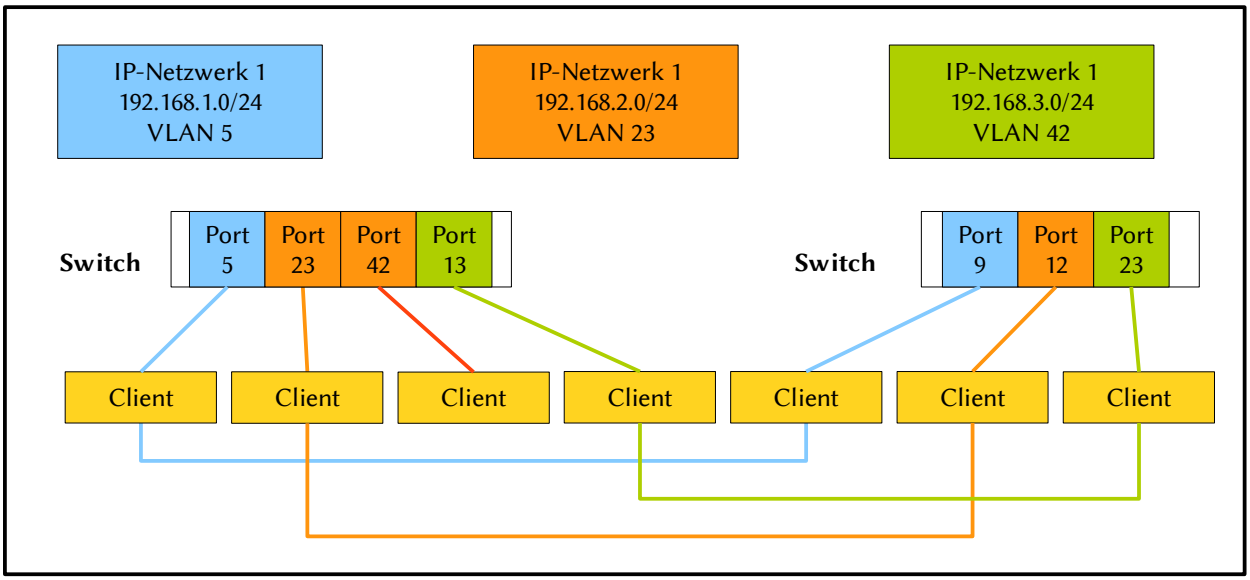


Abbildung 7: VLAN

Vorteil: Die Zugehörigkeit zu einem IP-Netzwerk kann pro Switch-Port festgelegt werden. Die Broadcasts sind auf die zugewiesenen Switch-Ports beschränkt...

14 DFS – Distributed File System

14.1 Eigenschaften

DFS trennt Pfadnamen und Speicherort

verwendet einen oder mehrere so genannte Root-Server, auf denen Sie die gewünschten virtuellen DFS-Links einrichten und festlegen, auf welche physikalischen Verzeichnis-Shares sie jeweils zeigen.

Benutzer greifen über einen logischen Pfadnamen auf Dateien zu, ohne zu wissen, wo diese physikalisch gespeichert sind.

Alles wird in einem Katalog gespeichert, per FRS (File Replication Service) wird dieser zwischen mehreren Servern synchronisiert.

14.2 Grundfunktion

Die Grundfunktion von DFS ist es, verschiedene Freigaben auf mehreren Servern zu einer Freigabe zusammenzufassen.

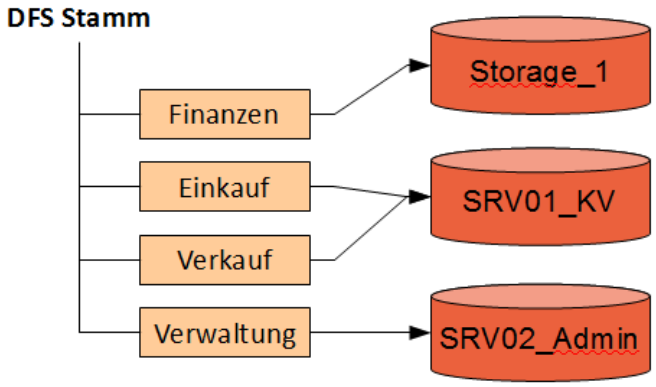
- Client ermittelt durch ActiveDirectory den nächstgelegenen DFS Root-Server. Ist ein DFS Root-Server nicht verfügbar, suchen die Clients einen weiteren.
- DFS leitet die Clients nun zu den DFS-Zielen (Targets), also den Servern mit den entsprechenden Freigaben. Wenn ein solcher Server ausfällt, leitet DFS die Clients zu einem Server, dessen Freigabe als DFS-Target für dieselbe DFS-Verknüpfung konfiguriert ist.

Der Client connectet zum DFS-Server. Dort schaut der Client, wo die eigentliche Freigabe ist, und connectet dann direkt darauf. Es passiert kein Umweg über den DFS-Server. Es muss nicht zwingend eine Windows-Freigabe sein (der Client muss das Protokoll einfach unterstützen).

Wenn ein AD vorhanden ist, erstellt man einen DFS-Domänenstamm.

DFS-Domänenstamm	\\domain.int\stammname
Eigenständiger Stamm	\\computername\stammname

14.3 Aufbau



Unterschiede der Stammarten

Domänen-DFS-Stamm (Normalfall)	Eigenständiger DFS-Stamm (selten)
verwendet das Active Directory (AD) zum Speichern der DFS-Konfiguration	Speicherung der Konf-Daten auf dem DFS-Server
automatische Dateireplikation (FRS)	Fehlertoleranz / Lastenausgleich auf Verknüpfungsebene (nur manuelle Replikation ohne NTFRS möglich)
freigegebene Ordner auf Stammebene möglich	keine freigegebenen Ordner auf Stammebene möglich
mehrere Verknüpfungsebenen möglich (Hierarchie)	nur eine Ebene von Verknüpfungen
DFS-Topologie wird automatisch im Active Directory veröffentlicht	Kein Links auf andere DFS
Muss auf Mitgliedserver der Domäne eingerichtet werden	

14.4 Vor- und Nachteile

Vorteile

- Einheitlicher Namespace
  - Unterschiedliche Freigaben können auf dasselbe Laufwerk gemappt werden, leitet aber für
  - User transparent auf eine beliebige Stelle im Netzwerk Einfachheit
- Verfügbarkeit der Dateien
  - File Replication Service
- Zuverlässigkeit des Dienstes
- Hohe Dienstzuverlässigkeit, weil Information über DFS Stamm im AD gepseichert wird
- Flexibilität

- Weniger Anpassungen bei Änderungen im Netzwerk
- Hohe Flexibilität bei Verzeichnisstrukturverwaltung
- UNC Pfad bleibt derselbe für User, Scripts etc., nur der DFS-Link muss angepasst werden im Hintergrund.
- Migration vereinfacht

Nachteil

- Verwaltungsaufwand

14.5 Voraussetzungen

OS	DFS-Client	DFS-Root	DFS-Ziel
W2k3	Ja	Ja	Ja
Windows XP	Ja	Nein	Ja
W2k Server	Ja	Ja	Ja
W2K Professional	Ja	Nein	Ja
Windows NT4 Server	Ja	Ja (kein Domain-Mode)	Ja
Windows NT4 Workstation	Ja	Nein	Ja
Windows 98	Ja (kein Domain Mode)	Nein	Ja

14.6 FRS (File Replication Service)

Das funktioniert nur beim **DFS-Domänenstamm** (setzt ActiveDirectory voraus).

Eine DFS-Verknüpfung kann auch auf mehrere Ziele Zeigen, die auf verschiedenen Servern liegen. (zwei Ziele)

Wenn eine DFS-Verknüpfung auf 4 Ordner zeigt, möchte man diese 4 Freigaben synchron halten! (Replikationssatz hinzufügen)

Bei Verwendung eines „eigenständigen DFS-Stammes“ (also ohne die Mitarbeit einer Domain) kann man zwar mehrere Ziele definieren, diese jedoch nicht automatisch synchronisieren (das muss dann anders gelöst werden.).

- Automatisch möglich
- Fehlertoleranz und ausfallsicherheit maximieren
- Ganzer DFS-Stamm oder nur DFS-Ordner

Automatische Replikation

- Nur auf Domänenstamm möglich
- NTFS ist erforderlich
- Passiert mit FRS
- Autoreplikation alle 15 Minuten
- Änderungen werden so immer repliziert zwischen DFS-Ordnern

Replikationsgruppe = Satz von Servern die an Replikation von einem oder mehreren DFS-Ordnern teilnehmen.

Replikationstopologie = Verbindungen zwischen den Servern die sich replizieren

14.7 Ausfallsicherheit

Sehr wichtig natüürli!!!

Klassischerweise verwendet man Cluster. Doch das DFS kann auch eine preisgünstigere Alternative sein.

DFS ist an zwei Stellen „empfindlich“: am DFS-Root (also die Anlaufstelle der Clients) und die DFS-Zeile (die Freigabe von den Servern).

So macht man es sicherer:

- DFS-Domänenstamm verwenden
- Redundante ActiveDirectory-Domainkontroller. Wenn kein DC vorhanden ist dann finden die Clients überhaupt nichts (/dev/null ☺).
- Redundante DFS-Roots: Wird über die MMC konfiguriert.
- Redundante DFS-Ziele: Mindestens 2 Ziele pro DFS-Verknüpfung. Diese sollten z.B. mit dem File Replication Service synchron gehalten werden.

Die redundanten Maschinen sollten physikalisch getrennt stehen…

14.8 Verteilen von Daten / Standortübergreifendes DFS

Damit die Mitarbeiter in Chur nicht über die WAN-Strecke auf den Server in Luzern zugreifen müssen, stellt man in Chur einen Server auf und erstellt eine Freigabe. Diese Freigabe definiert man dann als zusätzliches Ziel. Nun können die Mitarbeiter von Chur auf den Chur-Server zugreifen. Das macht man mit dem Domain Controller, dem DFS-Root und dem FileServer.

→ Man muss Das Datenvolumen beachten, damit die Synchronisation nicht die WAN-Strecke belastet.

14.9 Sicherung von Daten

Die verschiedenen Ziele auf den verschiedenen Lokationen werden mit dem FRS synchronisiert. Somit muss man nur an einem Ort einen Tape-Roboter aufstellen.

Sollte der Fileserver auf der Agentur ausfallen, so greifen die Clients auf die Daten im Hauptsitz

zu. Ein Störfallkonzept ist also schon integriert ;).

15 DHCP

15.1.1 DHCP – Vorgang

Folgendermassen läuft der Vorgang ab, wenn ein Client bei einem DHCP-Server eine IP-Adresse holt:

- **DHCPDISCOVER:** Ein Client ohne IP-Adresse sendet eine Broadcast-Anfrage nach Adress-Angeboten an den/die DHCP-Server im lokalen Netz.
- **DHCPOFFER:** Der/die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.
- **DHCPREQUEST:** Der Client fordert (eine der angebotenen) IP-Adresse(n), weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.
- **DHCPACK:** Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung

Es gibt noch andere DHCP-Meldungen:

- **DHCPNAK:** Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server
- **DHCPDECLINE:** Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.
- **DHCPRELEASE:** Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.
- **DHCPINFORM:** Anfrage eines Clients nach Daten ohne IP-Adresse, z. B. weil der Client eine statische IP-Adresse besitzt.

Eine 169.254.12.42 IP-Adresse gibt an, dass es einen Fehler gab! Der Client konfiguriert sich so selber.

15.1.2 DHCP-Relay-Agent[2]

Bei DHCP-Relay und BOOTP-Relay handelt es sich prinzipiell um den gleichen Mechanismus.

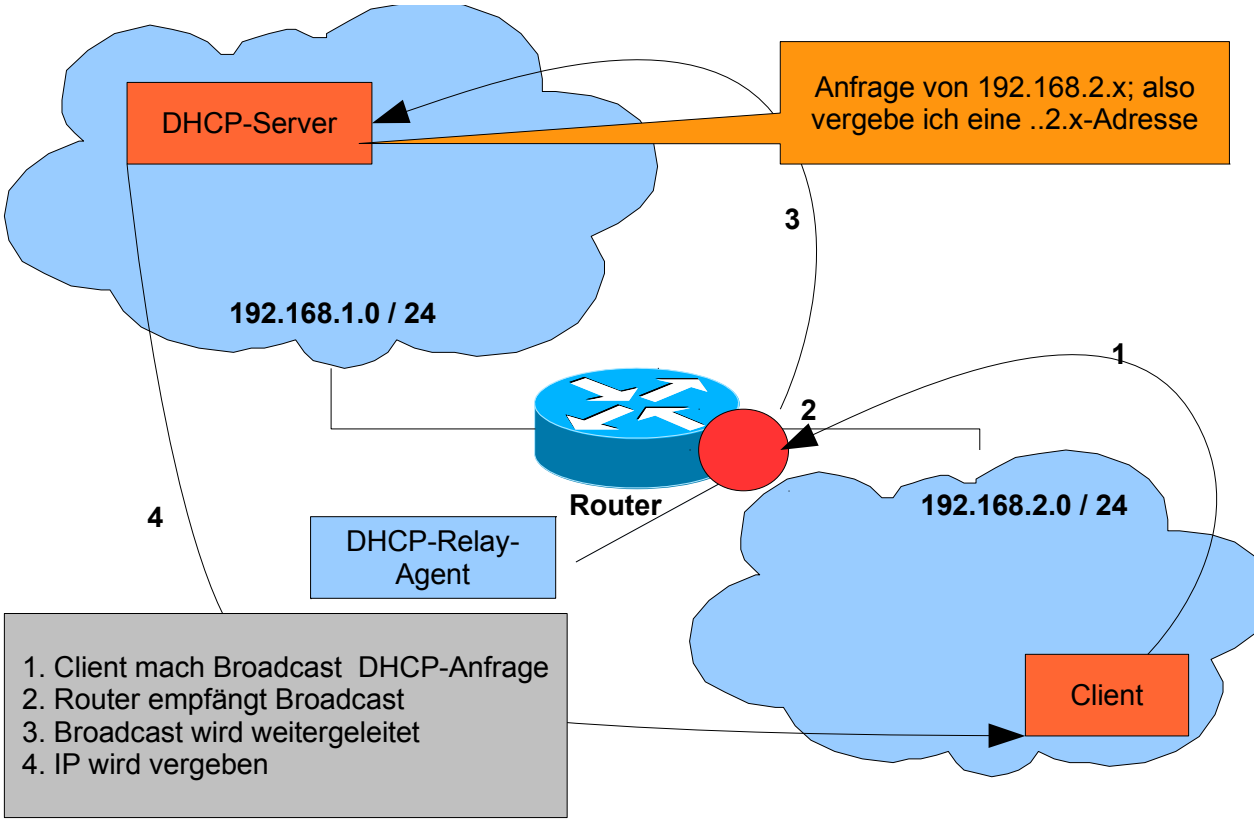
Die beiden Bezeichnungen werden oft synonym verwendet, besonders wenn es um Router-Eigenschaften geht.

Ein Router, der DHCP-Relay bzw. BOOTP-Relay beherrscht (ein sogenannter **RFC 1542-kompatibler Router**), kann **DHCP-Rundsendungen** (Broadcasts) aus einem seiner angeschlossenen Segmente an einen **DHCP Server weiterleiten, der in einem anderen Segment arbeitet.**

So können Rechner ihre IP-Adressen und -Parameter dynamisch übers Netzwerk erhalten, auch wenn kein **DHCP Server im gleichen Segment** steht (normalerweise würden die Broadcasts einen Router nicht überqueren).

Wenn der **Router diese Technik nicht beherrscht**, kann als Alternative auch auf einer NT- oder Windows 2000 -Maschine der **DHCP-Relay-Agent-Dienst aktiviert** werden.

Der Rechner mit diesem Dienst fängt dann DHCP-Broadcasts in seinem Segment auf und kann sie an einen DHCP-Server in einem anderen Segment weiterleiten.



2 Quelle: http://www.computerlexikon.com/begriff-dhcp-relay

16 NetBIOS

16.1.1 NetBIOS[3]

Namensauflösung

NetBIOS erlaubt einer Applikation, einen 16 Zeichen langen Namen netzwerkweit zu registrieren. Ursprünglich wurden die Zuordnungen von Namen zu Netzwerkadressen per Broadcast an alle Teilnehmer bekanntgegeben. Jeder NetBIOS-Name ist entweder als eindeutiger Name (exklusiv) oder als Gruppenname (nicht exklusiv) konfiguriert.

In Microsoft-Netzen werden von den 16 möglichen Zeichen 15 für Namen verwendet; das 16. Zeichen wird als Suffix benutzt, um verschiedene Dienste wie Server, RAS, Messenger usw. anzusprechen:

Rechnername + 00h	exklusiv	Arbeitsstationsdienst
Rechnername + 03h	exklusiv	Nachrichtendienst
Rechnername + 20h	exklusiv	Serverdienst
Benutzername + 03h	exklusiv	Name des angemeldeten Benutzers
Domänenname + 1Bh	nicht exklusiv	Name der Domäne, deren Mitglied der Rechner ist

(Wenn der Name aus weniger als 15 Zeichen besteht, wird er mit Leerzeichen aufgefüllt).

Verbindungsloser Datenaustausch (datagram service)

Die entsprechenden Funktionen realisieren die ungesicherte, paketweise Kommunikation zwischen zwei Endpunkten, ähnlich zu UDP im Internet. Der verbindungslos arbeitende Datagramm-Modus unterstützt einige Broadcast-Funktionen und bietet die Möglichkeit des Aufbaus virtueller Transportverbindungen sowie die Verwaltung symbolischer Namen für Endadressen. Dabei ist die Anwendung verantwortlich für die Aufrechterhaltung der Session.

Verbindungsorientierter Datenaustausch (session service)

Analog zu TCP bietet NetBIOS gesicherte, serialisierte Punkt-zu-Punkt Verbindungen an, d.h. es können Nachrichten übermittelt werden, die größer sind als die maximale Länge eines einzelnen Datenpaketes, und eventuell fehlerhaft angekommene oder verlorene Pakete werden erneut angefordert. Somit wird in diesem Modus eine Fehlererkennung und Fehlerkorrektur durchgeführt.

3 Quelle: Wikipedia

17 Capture-Filter

! oder not	Alles andere Erfüllt
&& oder and	Beide Bedingungen erfüllt
|| oder or	Nur eine Bedingung erfüllt
host $HOST	$HOST = 10.0.0.1 oder discordia
src host $HOST	
dst host $HOST	
port $PORT	$PORT = 23
src port $PORT	
dst port $PORT	
net $NET	$NET = 192.168 / Multicast: $NET=224.0.0
src net $NET	
dst net $NET	
ip oder ether proto \ip	Nur IP-Pakete
arp oder ether proto \arp	Nur ARP-Nachrichten
tcp oder ip proto \tcp	Nur TCP-Segmente
udp oder ip proto \udp or just udp	Nur UDP-Segmente
icmp oder ip proto \icmp	Nur ICMP-Nachrichten
tcp[0:2] = 80	Gehe zum Byte 0 und prüfe die nächsten zwei Bytes
icmp[0]= 0 or icmp[0]= 8	ICMP Ping

18 Tools

Ipconfig

ipconfig /all	DNS-Server anzeigen
ipconfig /flushdns	DNS-Cache löschen
ipconfig /displaydns	DNS-Cache anzeigen

netstat (Windows)

netstat [Optionen]

Option	Beschreibung
-a	Alle LISTEN
-e	Ethernet-Statistik
-n	Aktive TCP-Verbindungen
-o	Prozess-ID anzeigen
-p Protokoll	Nur Verbindungen mit dem angegebene Protokoll (z. B. tcp, udp, cimp, ip) anzeigen.
-s	Statisktik nach Protokollen anzeigen.
-r	Roitingtabelle anzeigen

tracert (Windows)

tracert [Optionen] zielhost

Option	Beschreibung
-d	Hostname nicht auflösen
-h $MAX	Maximale anzahl Hops (Default: 30)
-w $TIMEOUT	Zeitlimit in Millisekunden für eine Antwort (Default: 4000)
-6	IPv6 benutzen

ping (Windows)

ping [Optionen] ziel

Option	Beschreibung
-t	Pingen, bis manueller Abbruch (^C)
-a	Hostnamen mit DNS auflösen
-n $COUNT	Anzahl der Pings festlegen
-l	Grösse von „Optional Data“ (Bis 65'500; Default: 32)

-i $TTL	Time To Live (TTL) setzen (Default: 128)

route (Windows)

route

Option	**Beschreibung**
Print	Routing-Tabelle anzeigen
add $NETZID mask $SNMASK	Neuen Eintrag hinzufügen
-p add add $NETZID mask $SNMASK	Wird beim Reboot nicht gelöscht
change	Eine Route ändern
-f	Alle ausser die Standard-Routen löschen

nslookup

nslookup –type=mx edulu.ch	Mailserver von edulu.ch abfragen
nslookup –type=ns google.ch	Nameserver von Google.ch abfragen
nslookup –type=mx edulu.ch ns1.google.com	Mailserver von edulu.ch auf dem NS von Google abfragen

Interaktiver Modus

norecurse	Iterative Abfrage
lserver servername	Nameserver festlegen (ursprünglicher DNS-Server für Auflösung verwenden)
server servername	Nameserver festlegen (aktueller DNS-Server für Auflösung verwenden)
ls -d zone	Zonenübertragung (zuerst Server festlegen)
set type=xx	xx = abzufragender Ressource-Record

Zonenübertragung:

```
c:\tmp>nslookup
> server ns1.eris.org
Standardserver:  ns1.eris.org
Address:  23.5.42.3
> ls -d eris.org
```

18.1 Weitere Tools

dnscmd.exe	Anzeigen / Verändern von DNS-Einträgen, Zonen, Ressource Records
dnslint.exe	DNS-Diagnosetool

19 Portliste

Nr.	Dienst	Beschreibung
7	Echo	Zurücksenden empfangener Daten
20	FTP-Data	Dateitransfer (Datentransfer vom Server zum Client)
21	FTP	Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client)
22	SSH	Secure Shell
23	Telnet	Terminalemulation
25	SMTP, ESMTP	E-Mail-Versand (siehe auch Port 465)
42	Nameserver	Host Name Server (TCP und UDP)
43	Whois	Whois-Anfragen
53	DNS	Auflösung von Domainnamen in IP-Adressen
67	BOOTPS	BootStrap Protokoll server, auch genutzt von DHCP-Anfrage
68	BOOTPC	BootStrap Protokoll client, auch genutzt von DHCP-Antwort
80	HTTP	Webserver
110	POP3	Client-Zugriff für E-Mail-Server
119	NNTP	Usenet (Newsgroups)
123	NTP	Zeitsynchronisation zwischen Computern
143	IMAP	Zugriff und Verwaltung von Mailboxen
161	SNMP (UDP)	Überwachung und Steuerung von Netzwerkelementen
443	HTTPS	Verschlüsselte Webserver Übertragung, meist mit SSL- oder TLS-Verschlüsselung
445	Microsoft-DS	Microsoft Directory Server, Windows Dateifreigabe, SMB
465	SMTPS	gesicherter E-Mail-Versand
993	IMAPS	gesicherter Zugriff und Verwaltung von Mailboxen
995	POP3S	gesicherter Client-Zugriff für E-Mail-Server
1723	PPTP	Point-to-Point Tunneling Protocol VPN
3306	MySQL	Zugriff auf MySQL-Datenbanken
3389	RDP	Windows Remotedesktopzugriff, Windows Terminal Services
5060	SIP	IP-Telefonie
5800	VNC	Virtual Network Computing (Port für Java-Zugriff)
5900	VNC	Virtual Network Computing (Port für VNC Viewer-Zugriff)
6667	IRC	Chatserver
10000	Webmin	Webmin - Web-basierende Oberfläche für Systemadministratoren unter Linux
20000	Usermin	Oberfläche für Systemadministratoren unter Linux (ähnlich Webmin)

Weitere Informationen

- http://emanuelduss.ch
  Weitere Zusammenfassungen, Dokumentationen und Dokumente von mir

Glossar

Begriff	Definition

Stichwortverzeichnis